DSLink®
220
Conexão Banda Larga ADSL

Manual do Usuário

www.dslink.com.br

Fabricado e comercializado sob licença exclusiva de Opticom Communications, LLC, 1050 Connecticut Avenue, NW, Suite 1000, Washington DC 20036, USA, ☎ +1 202 772-4291, www.opticom.co.il. A Opticom Communications reserva-se o direito de melhorar, aprimorar e modificar os recursos e especificações de seus produtos sem prévia notificação. © Copyright 2001-2005. Todos os direitos autorais reservados. A duplicação, uso ou distribuição não autorizada constitui uma violação das leis aplicáveis. Todas as marcas são registradas e pertencem aos seus respectivos proprietários. Fotos meramente ilustrativas. 050726

Nenhuma parte desta publicação poderá ser reproduzida seja de que forma for sem a permissão escrita anterior. Outras marcas comerciais ou marcas registradas mencionadas neste documento são marcas comerciais ou marcas registradas de suas respectivas empresas.

Revisão 2.6

Julho 2005

Índice

1 Introdução 1

Características 1
Conteúdo da caixa do produto 1
Requisitos do Sistema 2

2 Hardware e Conexão 3

Painel Frontal 3
Painel Traseiro 3
Conectando o Hardware 4
Passo 1. Conecte-se à tomada telefônica 4
Passo 2. Conecte-se a um PC ou hub/switch. 5
Passo 3. (Opcional) Conecte-se a um PC USB. 5
Passo 4. Ligue o conector PWR. 5
Passo 5. Ligue o DSLink 220 e energize seus sistemas. 5

3 Usando um PC conectado à porta USB 7

Configurando um PC conectado à porta USB 7
Parte 1. Ligando o cabo USB. 7
Parte 2. Instalando o driver USB 7
Para Verificar a Instalação do Dispositivo USB 9
Para Remover o Driver USB 10

4 Configuração do PC Local 11

Configurando seus PCs como clientes DHCP 11
PCs com sistema operacional Windows® 95, 98 e Me: 11
Estações de trabalho Windows NT 4.0: 12
PCs com sistema operacional Windows 2000 e XP: 12
Para atribuir informações IP estáticas a seus PCs 13

5 Iniciando com o Configuration Manager 14

Acessando o Configuration Manager 14

Botões e Ícones Comumente Usados 14
Visualizando informações básicas do sistema..... 15
Efetivando Alterações para Armazenamento Permanente..... 16
Reinicializando o DSLink 220 com o uso do Configuration Manager..... 16
System Mode 17
Quick Configuration 17
Exemplos de Quick Configuration..... 20
RFC 1483 Bridge..... 20
RFC 1577 Router 21
RFC 2364 PPPoA 22

6 Configuração Básica..... 23

Modo Bridge..... 23
Parte 1: Configurando o DSLink 220..... 23
Parte 2: Verifique o status de sua conexão. 27
Parte 3: Configurando o PC. 27
Modo PPP Connection..... 28
Parte 1: Configurando o DSLink 220..... 28
Parte 2: Verifique o status de sua conexão. 30
Parte 3: Configurando o PC. 31
Modo Router Connection..... 31
Parte 1: Configurando o DSLink 220..... 31
Parte 2: Verifique o status de sua conexão. 33
Parte 3: Configurando o PC. 34

7 Configurando Rotas IP 35

Visualizando a Tabela de Roteamento IP 35
Adicionando Rotas IP 35

8 Configuração DHCP 37

Modos DSLink 220 DHCP 37
Configurando o Servidor DHCP 37
Parte 1. Criando pools de endereços IP..... 37
Parte 2. Ativando o Modo DHCP Server 39
Parte 3. Configurando seus PCs como clientes DHCP 39
Modificando Pools de Endereços..... 39
Visualizando Atribuições de Endereço DHCP Atuais..... 40
Configurando a Retransmissão DHCP 40
Parte 1. Definindo a(s) interface(s) de retransmissão DHCP 40

Parte 2. Ativando modo de retransmissão DHCP..... 41
Parte 3. Configurando seus PCs como clientes DHCP 41

9 Configuração NAT..... 42

Sua Instalação NAT Padrão 42
Visualizando Sua Configuração NAT 42
Visualizando Regras NAT e Estatísticas de Regras 45
Visualizando Conversões NAT Atuais..... 45
Adicionando Regras NAT..... 46
A regra napt: Efetuando conversões entre endereços IP públicos e privados 46
A regra rdr: Permitindo acesso externo a um computador da LAN48
A regra basic: Executando conversões 1:1..... 49
A regra filter: Configurando uma regra basic com critérios adicionais..... 50
A regra bitmap: Executando conversões bidirecionais..... 52
A regra PASS : Permitindo que endereços específicos passem sem conversão..... 53

10 Configurando Endereços do Servidor DNS e DDNS..... 54

Visão Geral da Retransmissão DNS 54
Configurando a Retransmissão DNS 54
Configurando DDNS 56

11 Configuração RIP 57

Configurando o RIP 57
Visualizando Estatísticas do RIP 58

12 Firewall, Filtros de IP, Filtro de Bridge e Bloqueio de Protocolos..... 60

Configurando o Firewall 60
Configurando Definições Globais de Firewall 60
Configuração de IP Filter..... 62
Visualizando sua configuração de IP Filter..... 62
Configurando Definições Globais de IP Filter..... 63
Criando Regras de Filtros de IP..... 64
Exemplos de regra filter de IP 70

Visualizando Estatísticas de Filtros de IP 70
Gerenciando Sessões Atuais de Filtros IP 71
Configuração de Bridge Filter..... 72
Visualizando sua configuração de Bridge Filter..... 72
Configurando Definições Globais de Bridge Filter 72
Criando Regras de Filtros Bridge..... 73
Visualizando Estatísticas de Filtros Bridge 74
Para bloquear protocolos específicos..... 74

13 Tarefas de Administração 76

Alterando a data e hora do sistema 76
Adicionando um usuário/Alterando sua senha de logon..... 76
Atualização da imagem..... 77
Diagnósticos 78
Configurações de portas 79
Visualização dos alarmes do sistema..... 79
Sistema de Log..... 80
Backup / Restore da Configuração 80
Autodetect..... 81
Configuração SNMP..... 81

14 Visualização dos parâmetros DSL 82

15 Solução de problemas..... 84

1 Introdução

Parabéns por ter adquirido o roteador/ bridge DSLink 220. Sua LAN (rede local) agora será capaz de acessar a Internet usando sua conexão ADSL de alta velocidade.

Este manual lhe mostrará como instalar e configurar seu DSLink 220 e como personalizar sua configuração para obter o máximo de seu novo produto.

Características

- Modem ADSL externo para acesso à Internet em alta velocidade
- Roteador Ethernet 10/100Base-T para proporcionar conectividade com a Internet a todos os computadores de sua LAN
- Porta USB para conexão a um PC com porta USB
- Funções de conversão de endereços de rede (NAT) e de filtragem de IP para proporcionar proteção por firewall para seus computadores
- Configuração da rede através de DHCP
- Programa de configuração que pode ser acessado por meio de um navegador HTML

Conteúdo da caixa do produto

Seu DSLink 220 deve chegar com o seguinte:

- Um roteador ADSL
- Um cabo de força AC
- Uma fonte universal
- Um cabo de rede
- Um cabo telefônico
- Um cabo USB (para o DSLink 220U/E somente)
- Um CD com software e manual do usuário (este manual)
- Um manual de instalação rápida com termo de garantia
- Microfiltros (somente quando indicado na parte externa da embalagem)

Requisitos do Sistema

Para utilizar seu DSLink 220, será preciso o seguinte:

- Serviço ADSL funcionando corretamente em sua linha telefônica, com pelo menos um endereço de Internet público para sua LAN.
- Um ou mais computadores contendo uma placa de interface de rede (NIC) Ethernet 10Base-T/100Base-T e/ou um só computador com uma porta USB, quando usar o DSLink 220U/E.
- Um hub/switch Ethernet, caso esteja conectando o dispositivo a mais de um computador.
- Para a configuração do sistema usando o programa estilo Web fornecido: um navegador da Web como, por exemplo, Internet Explorer v5.0 ou posterior, ou Netscape v5.0 ou posterior.

2 Hardware e Conexão

Painel Frontal

O painel frontal contém indicadores denominados LEDs, que indicam o status da unidade.

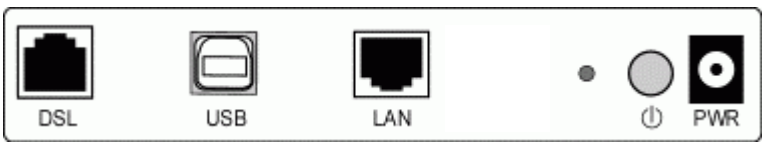
DSLink 220U/E

DSLink 220E

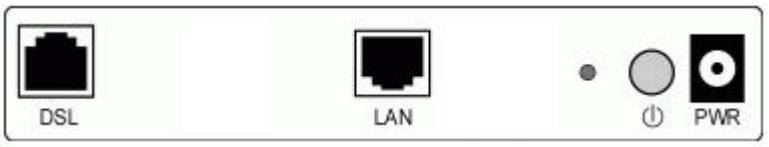
Identificação	Cor	Função
PWR	verde	Aceso: A unidade está ligada Apagado: A unidade está desligada
DIAG	verde	Pisca acendendo-se e apagando-se para indicar que o software do dispositivo está operacional. Apaga-se após 10-15 segundos.
LAN	verde	Aceso: Enlace LAN estabelecido e ativo Apagado: Sem enlace LAN
ACT	verde	Pisca quando ocorre atividade de dados ADSL. Pode ficar continuamente aceso quando o tráfego de dados é intenso.
DSL	verde	Aceso: Enlace ADSL estabelecido e ativo Apagado: Sem enlace ADSL
USB (opcional)	verde	Aceso: Enlace USB estabelecido Apagado: Sem enlace USB

Painel Traseiro

O painel traseiro contém as portas para as conexões de dados e de alimentação da unidade. As funções estão descritas conforme abaixo (da esquerda para a direita):



DSLink 220U/E



DSLink 220E

Identificação	Função
DSL	Conecta o dispositivo a uma tomada de telefone ADSL usando o cabo fornecido
USB (opcional)	Conecta-se à porta USB de seu PC
LAN	Conecta o dispositivo à porta Ethernet de seus PCs, ou à porta uplink do hub de sua LAN, usando o cabo fornecido
Reset Button	Redefinição para os padrões de fábrica. Para redefinir o dispositivo para os padrões de fábrica, não é necessário desligar o dispositivo. Basta introduzir um clipe de papéis no orifício. Pressione o botão 3 vezes e, em seguida, solte. Depois, aguarde o dispositivo terminar a inicialização.
⏻	Liga e desliga a unidade
PWR	Conecta-se à saída da fonte DC fornecida

Conectando o Hardware

Siga os procedimentos abaixo para conectar dispositivos relacionados. Antes de começar, desligue a alimentação de todos os dispositivos. Estes incluem seu(s) computadores e o DSLink 220.

Passo 1. Conecte-se à tomada telefônica

Conecte uma extremidade do cabo telefônico RJ11 à porta identificada como **DSL** no painel traseiro do dispositivo. Conecte a outra extremidade à sua tomada telefônica com serviço ADSL.

Nota

Dependendo do tipo de serviço oferecido por seu ISP, poderá ser necessário um divisor adicional. Se este for o caso, consulte seu ISP para informações sobre a conexão efetiva.

Passo 2. Conecte-se a um PC ou hub/switch.

- A um único PC – Conecte uma extremidade de um cabo Ethernet “direto” à porta identificada como **LAN** e a outra extremidade à porta Ethernet de seu PC.
- A um hub/switch - Conecte uma extremidade de um cabo Ethernet “cruzado” **(não fornecido)** a um hub/switch e a outra extremidade à porta LAN do DSLink 220.
- A uma porta uplink do hub/switch: - Use um cabo “direto” para conectá-lo à porta uplink e o outro para a porta **LAN** do DSLink 220.

Passo 3. (Opcional) Conecte-se a um PC USB.

Para conectar-se a um único PC por meio da porta USB, você deve conectar primeiro o cabo USB e então instalar no PC o driver USB fornecido.

. Siga as instruções descritas no capítulo 3 deste manual, no item **“Usando um PC conectado à porta USB”**

Nota

Para usar a interface USB, seu micro deve ter instalado o Windows ® 98SE/ME, 2000 ou XP.

Passo 4. Ligue o conector PWR.

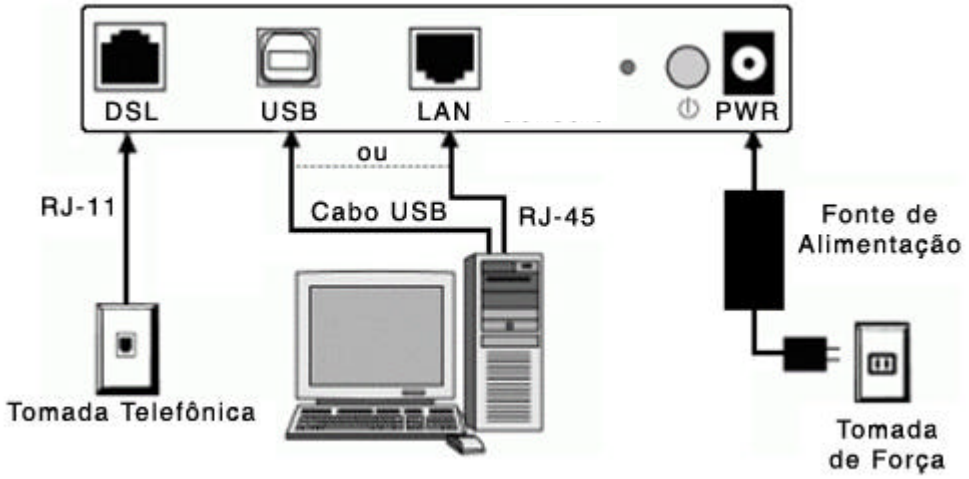
Conecte a saída da fonte DC ao conector **PWR** na parte traseira do dispositivo e a entrada da fonte, através do cabo de força, a uma tomada de parede ou régua de alimentação.

Passo 5. Ligue o DSLink 220 e energize seus sistemas.

Pressione a chave liga/desliga no painel traseiro do dispositivo para ligá-lo.

Ligue e inicialize seu(s) computador(es) e quaisquer dispositivos LAN.

O diagrama abaixo ilustra um exemplo de conexão:


DSL
USB
LAN
PWR
ou
RJ-11
Cabo USB
RJ-45
Fonte de
Alimentação
Tomada Telefônica
Tomada
de Força

3 Usando um PC conectado à porta USB

NOTA: Se você estiver usando o DSLink 220E, pule este capítulo.

Este capítulo descreve as instruções para usar um PC conectado à porta USB do DSLink 220 U/E. Se seu computador não tem uma porta USB, ignore este capítulo.

Configurando um PC conectado à porta USB

Se você usa a porta USB do DSLink 220 U/E para se conectar a um PC, você deve conectar primeiro o cabo USB e então instalar o driver USB fornecido no PC. O driver ativa a comunicação Ethernet-sobre-USB com o DSLink 220 U/E. Certifique-se de seguir os passos descritos abaixo

As telas descritas abaixo são basicamente as mesmas para Windows ® 98SE/ME, 2000 e XP. As telas mostradas são para o Windows 2000.

Parte 1. Ligando o cabo USB.

Ligue o cabo USB ao DSLink 220 U/E e ao seu PC.

Depois de ligar o cabo USB, a função plug-and-play do Windows iniciará o assistente de instalação de hardware solicitando um driver USB. Clique em **Cancel** para pular esta tela.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install a device driver for a hardware device.
To continue, click Next.
< Back
Next >
Cancel

Parte 2. Instalando o driver USB.

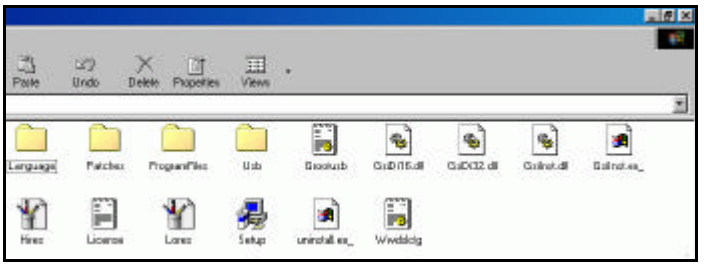
1. Coloque o CD de software fornecido no seu driver de CD-ROM.

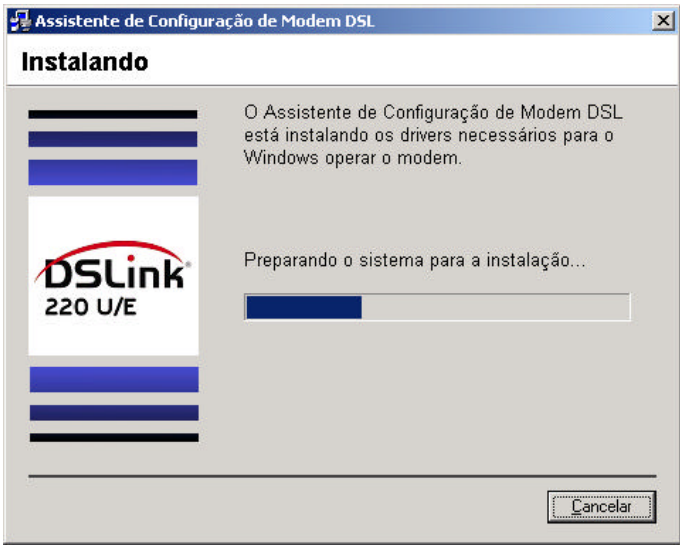
2. Localize os arquivos de instalação de USB no CD de software e clique duas vezes em **setup.exe** para iniciar o programa de instalação. O programa de instalação não é

específico para um sistema operacional; Windows 98SE/ME, 2000 e XP usam o mesmo programa de instalação.

Siga então as instruções na tela para instalar o driver de USB.

Para Windows 98SE/ME/2000/XP: Clique **Yes** ou **Continue Anyway** se aparecer a mensagem de certificação da Microsoft.




Assistente de Configuração de Modem DSL
Instalando
O Assistente de Configuração de Modem DSL está instalando os drivers necessários para o Windows operar o modem.
DSLink
220 U/E
Preparando o sistema para a instalação...
Cancelar

3. Se solicitado a reiniciar seu computador, clique em **Yes** para completar a instalação do driver de USB.

Para Verificar a Instalação do Dispositivo USB

Se você precisar verificar se o dispositivo USB está adequadamente instalado no seu PC, inicie o **Device Manager** como abaixo:

- No **Control Panel**, clique **System** > **Hardware** > **Device Manager**.

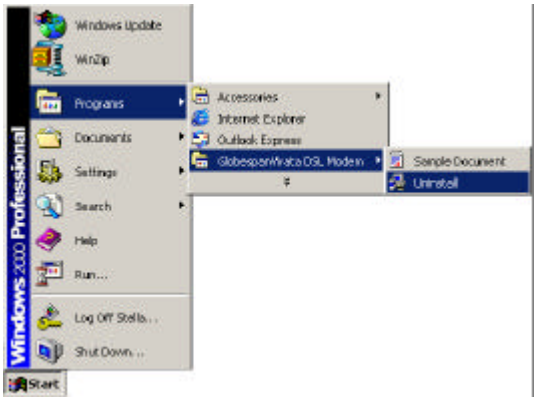
Na janela **Device Manager**, clique duas vezes em **Network adapters** para mostrar o adaptador **GlobespanVirata USB IAD LAN Modem**.

Se um ponto de exclamação aparecer perto do adaptador, seu adaptador USB não vai funcionar corretamente. Por favor desligue e depois religue o cabo USB para resolver este problema.

Se não aparecer o ponto de exclamação ao lado do adaptador USB, seu dispositivo USB estará funcionando corretamente.

Para Remover o Driver USB

Se você precisar remover o driver USB, por favor use o programa de desinstalação fornecido, selecionando **Start** > **Programs** > **DSLink220UE** > **Uninstall**. Siga então as instruções do sistema para continuar.



4 Configuração do PC Local

Por padrão, o DSLink 220 age como servidor DHCP e atribui automaticamente todas as configurações Internet necessárias a seus PCs, ou seja, os clientes DHCP.O endereço IP e o pool DHCP predefinidos são os seguintes:

	Porta LAN	**Porta USB**
Endereço IP	192.168.1.1	192.168.1.2
Máscara de sub-rede	255.255.255.0	255.255.255.0
Pool DHCP	192.168.1.3~252	192.168.1.2

Estas instruções partem do princípio de que seu PC satisfaz os seguintes pré-requisitos:

4. Já está conectado à porta LAN do dispositivo através de sua placa de interface de rede (NIC) ou conectado por meio da porta USB.

5. Possui o software de adaptador Ethernet apropriado (ou o driver USB, se estiver conectado por meio de porta USB).

6. O protocolo TCP/IP está instalado. Em caso negativo, consulte a documentação da Microsoft para instalar o TCP/IP.

É preciso apenas configurar os PCs para aceitarem as informações quando elas forem transferidas. Siga as instruções que correspondam ao sistema operacional instalado em cada PC.

Configurando seus PCs como clientes DHCP

PCs com sistema operacional Windows® 95, 98 e Me:

1. Na barra de tarefas do Windows, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.

2. Clique duas vezes no ícone **Rede**.

3. Na guia **Configuração**, selecione a rede TCP/IP associada à sua placa de rede e, em seguida, clique em **Properties**.

   Nota: Se estiver usando PC USB, selecione o TCP/IP relativo ao seu dispositivo USB, p.ex., *GlobeSpan USB ADSL LAN Modem***.**

Nota

Para usar a interface USB, seu micro deve ter instalado o Windows® 98SE/ME, 2000 ou XP.

4. Na caixa de diálogo Properties de TCP/IP, clique na guia **Endereço IP**.

5. Clique no botão de opção identificado como **Obtain an IP Address Automatically**.

6. Clique em **OK** duas vezes para confirmar e salvar suas alterações.

7. Será solicitado salvar o Windows. Clique em **Sim**.

Estações de trabalho Windows NT 4.0:

1. Na barra de tarefas do Windows NT, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.

2. Na janela Painel de controle, clique duas vezes no ícone **Rede**.

3. Na caixa de diálogo Rede, clique na guia **Protocols**.

4. Na guia **Protocols**, selecione **TCP/IP** e, em seguida, clique em **Properties**.

5. Na caixa de diálogo **Properties** de TCP/IP Microsoft, clique no botão de opção identificado como **Obter um endereço IP de um servidor DHCP**.

6. Clique **OK** duas vezes para confirmar e salvar suas alterações e, em seguida, feche o Painel de controle.

Nota

Para usar a interface USB, seu micro deve ter instalado o Windows ® 98SE/ME, 2000 ou XP.

PCs com sistema operacional Windows 2000 e XP:

1. Na barra de tarefas do Windows, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.

2. Clique duas vezes no ícone **Conexões de rede e dial-up** (ou **Conexões de rede** para o Windows XP).

3. Clique com o botão direito do mouse no ícone **Conexão local** e, em seguida, selecione **Properties**.

4. Realce **Internet Protocol (TCP/IP)** e, em seguida, clique em **Properties**.

   Nota: Se estiver usando PC USB, selecione o TCP/IP de seu dispositivo USB, por exemplo: *GlobeSpan USB ADSL LAN Modem***.**

5. Na caixa de diálogo **Internet Protocol Properties (TCP/IP)**, clique no botão de opção identificado como **Obtain an IP Address Automatically**. Clique também no botão de opção identificado como **Obtain DNS server address**.

6. Clique em **OK** duas vezes para confirmar e salvar suas alterações e, em seguida, feche o Painel de controle.

Para atribuir informações IP estáticas a seus PCs

Em alguns casos, você pode querer atribuir IP estático a seu PC diretamente se:

- No modo **bridge**, está concluída a configuração inicial e será preciso usar o endereço IP e o gateway fornecidos por seu ISP.
- Foi obtido um ou mais endereços IP públicos que quer associar sempre a computadores específicos (por exemplo, se estiver usando um computador como servidor de rede público).
- São mantidas diferentes sub-redes em sua LAN.

Antes de começar, entre em contato com seu ISP caso não tenha as seguintes informações:

- Endereço IP e máscara de sub-rede.
- Gateway padrão.
- Servidor DNS.

Em cada PC ao qual queira atribuir informações estáticas, siga as instruções para a exibição de cada uma das propriedades TCP/IP. Em vez de ativar a atribuição dinâmica dos endereços IP relativos ao computador, clique nos botões de opção que permitem inserir manualmente o endereço IP, o DNS e o gateway padrão.

5 Iniciando com o Configuration Manager

Seu DSLink 220 inclui um *Configuration Manager* com interface Web, que possibilita configurar as definições do dispositivo para que satisfaçam as necessidades de sua rede.

Acessando o Configuration Manager

O programa pode ser acessado de qualquer computador conectado ao DSLink 220 por meio de portas LAN (ou USB no caso do DSLink 220U/E).

1. Em um computador da LAN, abra seu navegador da Web, digite o seguinte URL na caixa de endereço (ou localização) e pressione **<Enter>**:

   `http://192.168.1.1`

   Ou, a partir do computador com interface USB, quando usando o DSLink 220 U/E, digite:

   `http://192.168.1.2`

   Estes são os endereços IP predefinidos das portas LAN e USB em seu DSLink 220 U/E.

2. Quando a tela de logon for exibida, digite seu nome do usuário e senha e, em seguida, clique em **OK**.

   Na primeira vez que iniciar o programa, use estes valores padrão:

   Default User Name: root
   Default Password: root

   Após um logon bem-sucedido, é exibida a página **System View**.

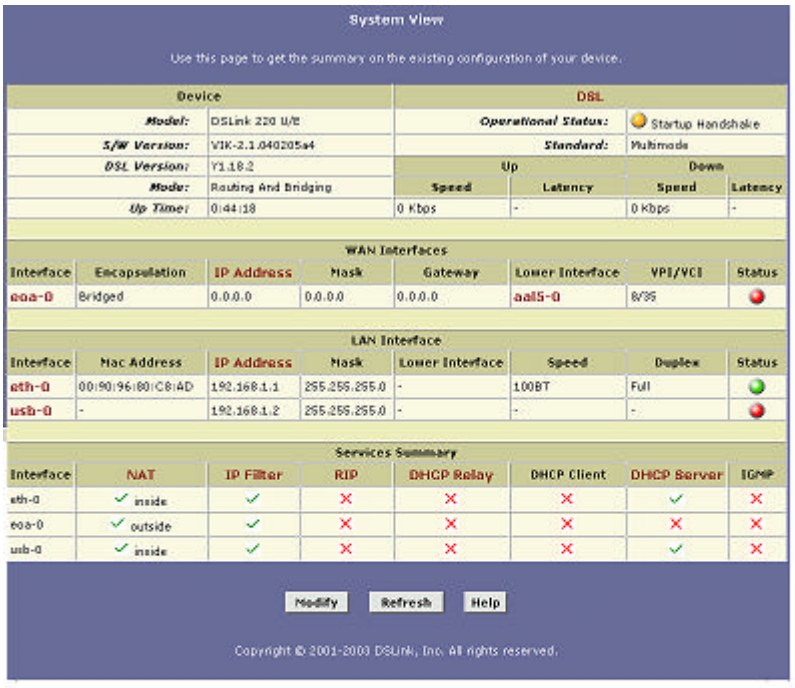
Botões e Ícones Comumente Usados

Botão	Função
Submit	Armazena na memória temporária do sistema quaisquer alterações feitas na página atual.

Botão	Função
Refresh	Reexibe a página atual com estatísticas atualizadas.
Clear	Quando estiverem sendo exibidas estatísticas acumuladas, este botão redefine as estatísticas para seus valores iniciais.
Help	Inicia a ajuda on-line relativa ao tópico atual em uma janela do navegador separada. A ajuda está disponível na página de qualquer tópico principal.
	Excluir uma entrada.
	Modificar uma entrada.
	Visualizar detalhes de uma entrada.

Visualizando informações básicas do sistema

A página System View é exibida ao acessar pela primeira vez o programa ou ao clicar na aba **Home**:



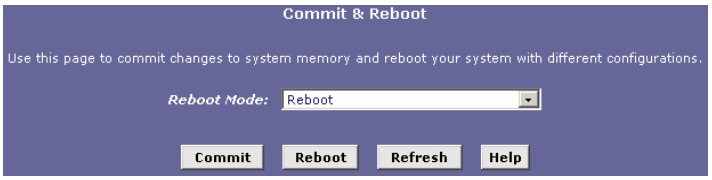
A tabela System View fornece um instantâneo da configuração de seu sistema. Pode-se clicar nos links fornecidos que permitem configurar cada definição (se disponível). Consulte os capítulos apropriados neste documento para obter mais informações.

Efetivando Alterações para Armazenamento Permanente

Sempre que forem alteradas as definições do sistema, as alterações são colocadas inicialmente em armazenamento temporário (denominado memória de acesso aleatório ou RAM). Suas alterações tornam-se efetivas quando são enviadas, mas serão perdidas se o dispositivo for redefinido ou desligado.

Siga estes passos para efetivar alterações para armazenamento permanente.

1. Selecione **Admin** > **Commit & Reboot**. É apresentada a página Commit & Reboot:



2. Clique em **Commit**. (Desconsidere a seleção na lista suspensa Reboot Mode; ela não afeta o processo de efetivação).

   As alterações são salvas no armazenamento permanente.

Quando efetivar suas alterações, observe que:

- Se for alterar as informações de endereço IP da LAN, **deverá** efetivar as alterações e, em seguida, reinicializar o sistema para ativá-las.
- Todas as outras alterações são ativadas quando forem efetivadas (nenhuma reinicialização é necessária).

Reinicializando o DSLink 220 com o uso do Configuration Manager

Se, após reinicializar o DSLink 220, for descoberto que ele não funciona corretamente com a nova configuração, poderá reinicializá-lo usando as opções que ativarem novamente uma configuração anterior ou a configuração padrão do fabricante.

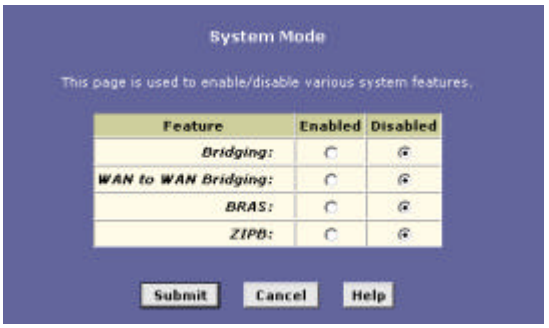
É possível selecionar entre as três opções a seguir quando da reinicialização:

Definição	Descrição
Reboot	Reinicializa o dispositivo para ativar suas novas definições (se houver).
Reboot from Last Configuration	Reinicializa o dispositivo usando as definições atuais na memória permanente, incluindo quaisquer alterações que foram recém efetivadas.
Reboot from Backup Configuration	Reinicializa o dispositivo usando as definições armazenadas na memória de backup. Estas são as definições que estavam em vigor antes de terem sido

Definição	Descrição
	efetivadas as novas definições na sessão atual.
Reboot from Default Configuration	Reinicializa o dispositivo para definições padrão fornecidas por seu ISP ou pelo fabricante. A escolha desta opção apaga qualquer definição personalizada.

System Mode

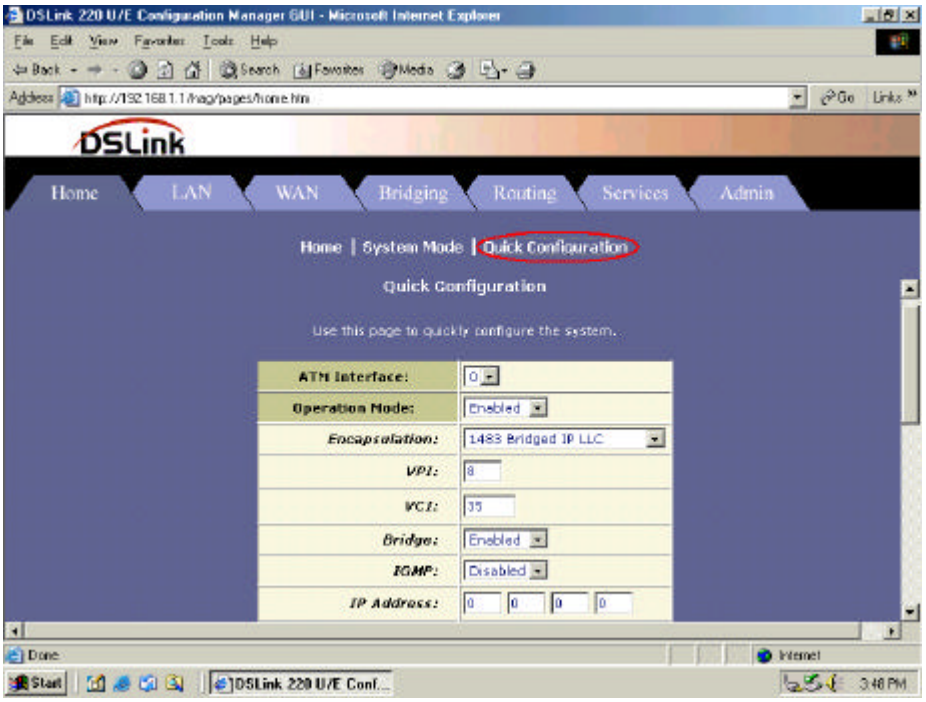
A página **System Mode** é usada para configurar o modo de operação de cada uma das interfaces criadas. Esta página deve ser usada em conjunto com a tela de **Bridge Configuration,** conforme descrito no item 3 do capítulo 6 deste manual.



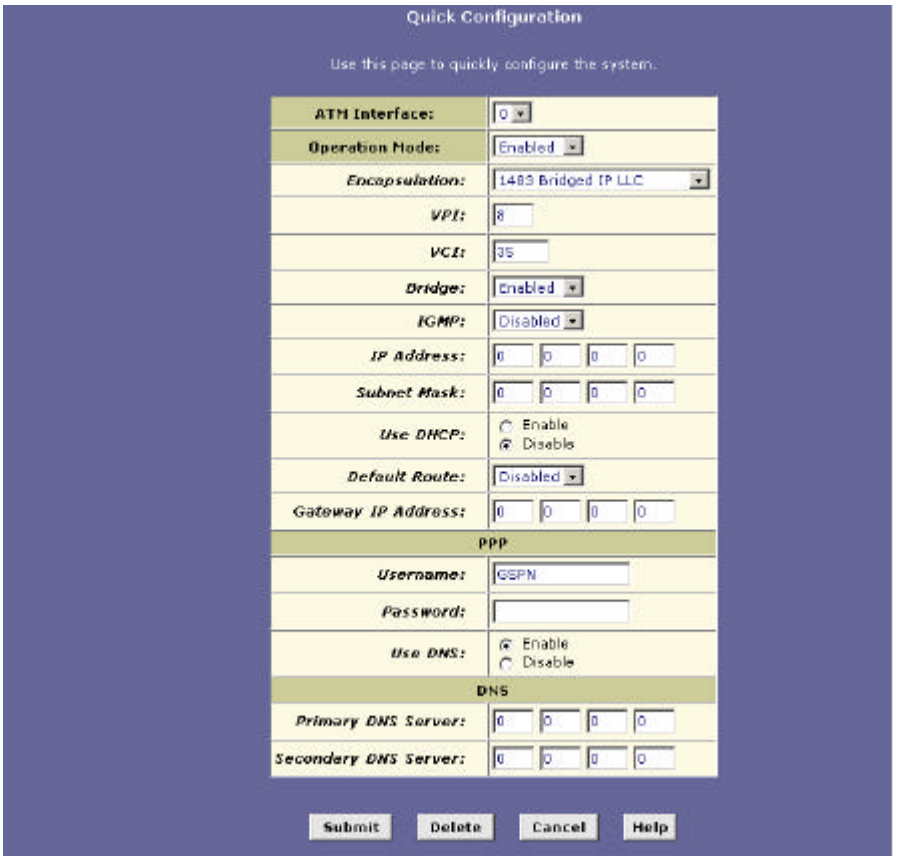
Quick Configuration

A página **Quick Configuration** permite que seu DSLink 220 seja configurado com rapidez para conexão à Internet. Seu ISP deve lhe fornecer as informações necessárias para a conclusão da configuração rápida.

NOTA: Algumas versões do Configuration Manager não incluem a opção **Quick Configuration**. Se na tela inicial do Configuration Mananger mostrada abaixo não aparecer a opção assinalada **Quick Configuration**, a configuração de seu DSLink 220 deve ser feita através das telas específicas para cada parâmetro, conforme descrito no Capítulo 6 deste manual.



Para configurar rapidamente o sistema, vá para **Home** > **Quick Configuration**. É exibida a página Quick Configuration.



Insira os campos fornecidos conforme abaixo.

Campo	Descrição
ATM Interface	Selecione a interface ATM que deseja usar (geralmente **atm-0**) para esta conexão.

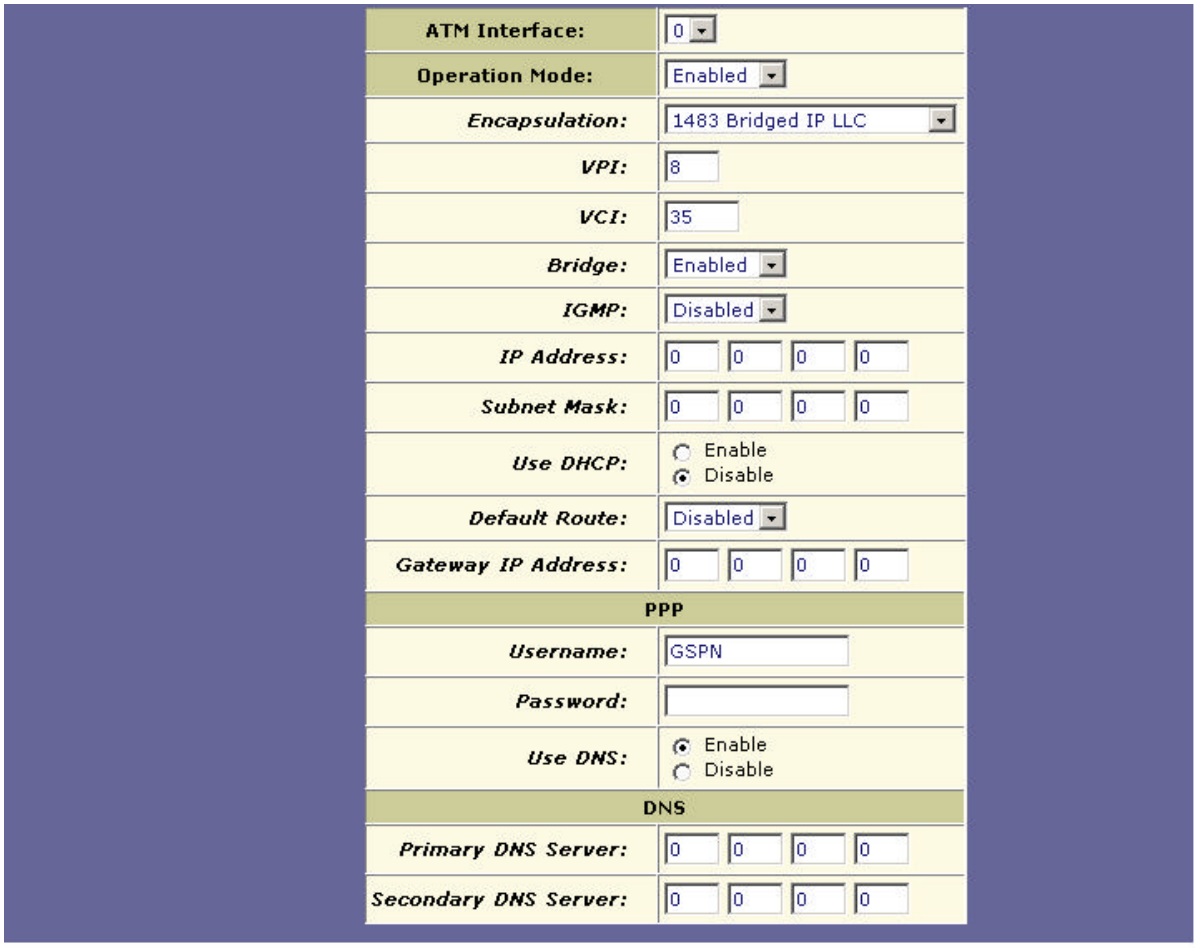
Operation Mode	Selecione **Yes**. Se definido como **No**, o dispositivo não poderá fornecer conectividade com a Internet para sua rede.
Encapsulation	Selecione o tipo de conexão que seu ISP utiliza para comunicar-se com seu DSLink 220.
VCI e VPI	Digite os valores VPI/VCI fornecidos por seu ISP.
Bridge	Esta definição ativa ou desativa a ponte entre o DSLink 220 e seu ISP. Seu ISP pode também referir-se a isto usando “RFC 1483” ou “Ethernet no ATM”.
IGMP	Esta definição ativa ou desativa o Internet Group Management Protocol. Entre em contato com seu ISP sobre ativar ou não esta definição.
IP Address e *Subnet mask*	Se seu ISP tiver atribuído um endereço IP público à sua LAN, digite o endereço IP e a máscara de sub-rede associada nas caixas fornecidas. Do contrário, mantenha o padrão 0.0.0.0/0.0.0.0.
Default Route	Quando desativada, o endereço IP especificado acima será usado como rota padrão para sua LAN
Gateway IP Address	Especifica o endereço IP que identifica o servidor do ISP através do qual sua conexão com a Internet será roteada.
User Name e *Password*	Caso selecionado o PPP como o tipo de Encapsulamento, digite o nome do usuário e a senha que usará para o logon em seu ISP.
Use DNS	Clique em Enable para ativar o serviço de encaminhamento de DNS, que encaminha para seus PCs da LAN o endereço do servidor DNS que sua conexão PPP obteve do seu ISP. Esta opção só pode ser usada quando o Roiteador/Bridge atua como um servidor DHCP para a sua LAN.
Primary/ Secondary DNS Server	É possível apenas manter o padrão 0.0.0.0. Caso sejam digitados os endereços DNS Primário e Secundário fornecidos por seu ISP, estes servidores DNS serão utilizados além de quaisquer servidores DNS descobertos automaticamente.

Após concluir as definições necessárias, clique em **Submit**.

Em seguida, vá para **Admin** > **Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

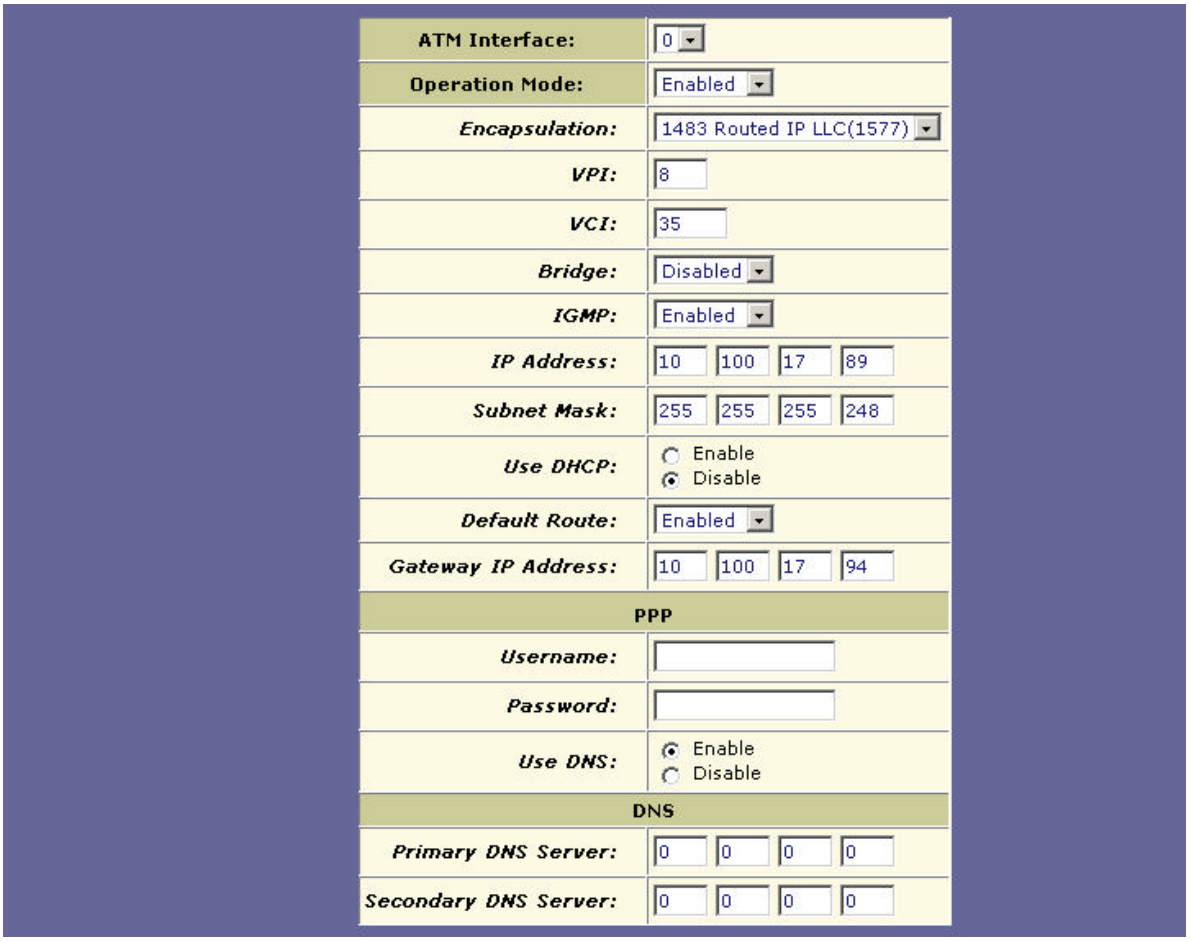
Exemplos de Quick Configuration

RFC 1483 Bridge



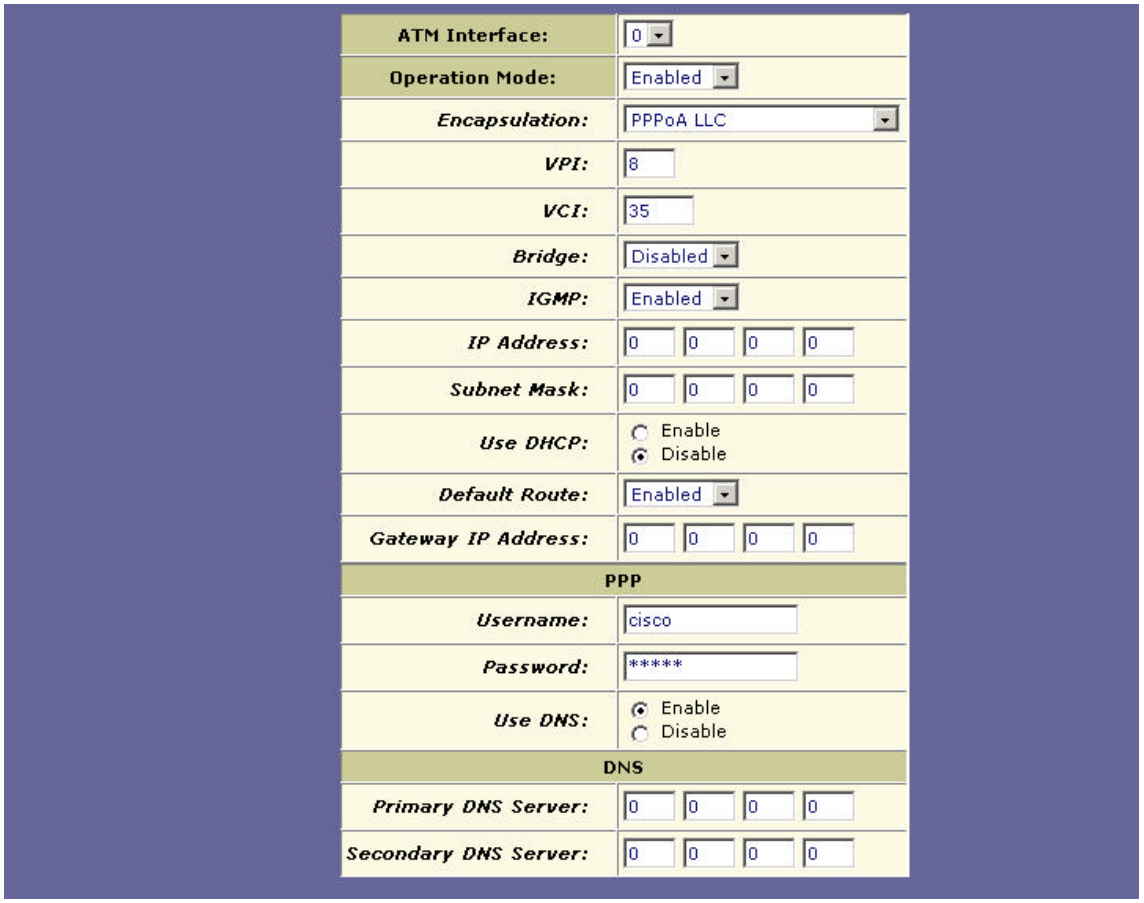
ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	1483 Bridged IP LLC
VPI:	8
VCI:	35
Bridge:	Enabled
IGMP:	Disabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Use DHCP:	○ Enable ◉ Disable
Default Route:	Disabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	GSPN
Password:	
Use DNS:	◉ Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

RFC 1577 Router



ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	1483 Routed IP LLC(1577)
VPI:	8
VCI:	35
Bridge:	Disabled
IGMP:	Enabled
IP Address:	10 100 17 89
Subnet Mask:	255 255 255 248
Use DHCP:	Enable / Disable
Default Route:	Enabled
Gateway IP Address:	10 100 17 94
PPP	
Username:	
Password:	
Use DNS:	Enable / Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

RFC 2364 PPPoA



6 Configuração Básica

Este capítulo fornece as configurações básicas para fazer com que seu dispositivo funcione e que sua rede seja conectada à Internet. As instruções partem do princípio de que o dispositivo não está predefinido com nenhuma configuração ATM VCC, PPP e IPoA. Para cada método de conexão, são fornecidos parâmetros de exemplo para uma melhor compreensão. Deve ser consultado seu ISP para determinar seu modo de conexão e digitar os valores reais fornecidos por seu ISP.

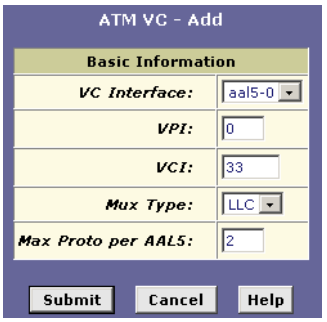
Seu dispositivo pode já estar pré-configurado com as definições necessárias para fazer com que sua rede seja conectada à Internet. Entre em contato com seu ISP para determinar se é necessário alterar algum valor existente.

Modo Bridge

Parte 1: Configurando o DSLink 220

1. Criando uma interface ATM VC.

a. Selecione **WAN** > **ATM VC** > **Add**. É exibida a página ATM VC-Add.



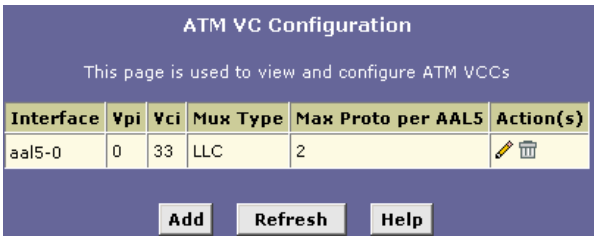
b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
VCC Interface	Selecione uma interface VCC entre as interfaces disponíveis, p.ex., ***aal5-0***.
VPI/VCI	Digite os valores VPI/VCI fornecidos por seu ISP, p.ex., ***0/33***.
Mux Type	Selecione **LLC** ou **VC** conforme o exigido por seu ISP.
Max Proto per AAL5	Mantenha o padrão.

Após digitar os campos acima, clique em **Submit**.

c. Quando aparecer a página de confirmação, clique em **Close**.

d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VC recém-adicionada.



2. Criando uma interface EoA.

a. Selecione **WAN** > **EoA** > **Add** para adicionar uma nova interface EoA.

b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
EOA Interface	Selecione uma interface EoA entre as interfaces disponíveis, p.ex., ***eoa-0***.
IPF Type	**Public**.
Lower Interface	Selecione a interface ATM VCC que foi criada no Passo 1, p.ex., ***aal5-0***.
Config. IP Address/Net Mask	**0.0.0.0**/**0.0.0.0**. Para usar o dispositivo como bridge, não é necessário definir o endereço IP e a máscara de sub-rede. Basta manter o padrão.
MTU	Maximum Transmission Unit (MTU) é o maior tamanho de

Campo	Descrição
	um pacote ou quadro, especificado em octetos (bytes de oito bits), que podem ser enviados em um pacote. O Internet's Transmission Control Protocol usa o MTU para determinar o tamanho máximo de cada pacote em qualquer transmissão.
Use DHCP	**Disable**
Default Route	**Disable**
Gateway IP Address	Deixe vazio. Não é preciso definir o gateway.

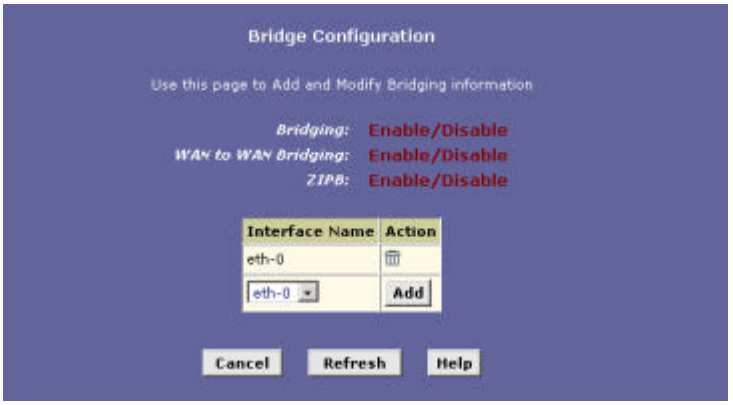
Após digitar os campos acima, clique em **Submit**.

c. Quando aparecer a página de confirmação, clique em **Close**.

d. Então retornará à tabela **EOA** e verá a entrada EOA recém-adicionada.

3. Ativação da função Bridging.

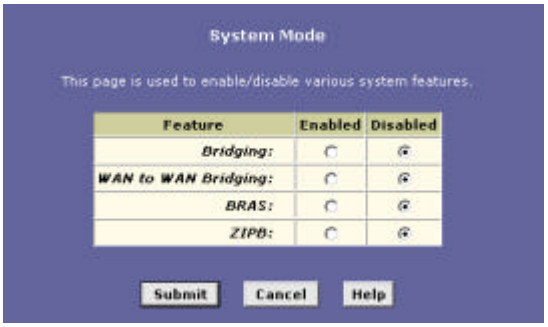
a. Selecione a aba **Bridging** para visualizar a página Bridge Configuration.



A página **Bridge Configuration** possui links (em vermelho) para a página **System Mode**, onde você pode ativar/desativar os serviços de bridging correspondentes. A página de **Bridge Configuration** também mostra uma tabela para especificar as interfaces que suportam bridging. A tabela pode estar vazia se não há ainda nenhuma interface configurada para bridging.

b. As interfaces **eth-0** e **usb-0** á devem estar adicionadas à tabela de bridge. Se não estiverem, selecione-as da lista e clique em **Add**.

c. Depois que você criou as interfaces você deve ativar os serviços de bridging no sistema como um todo. Clique na aba Home e depois em **System Mode**. A tela abaixo será mostrada

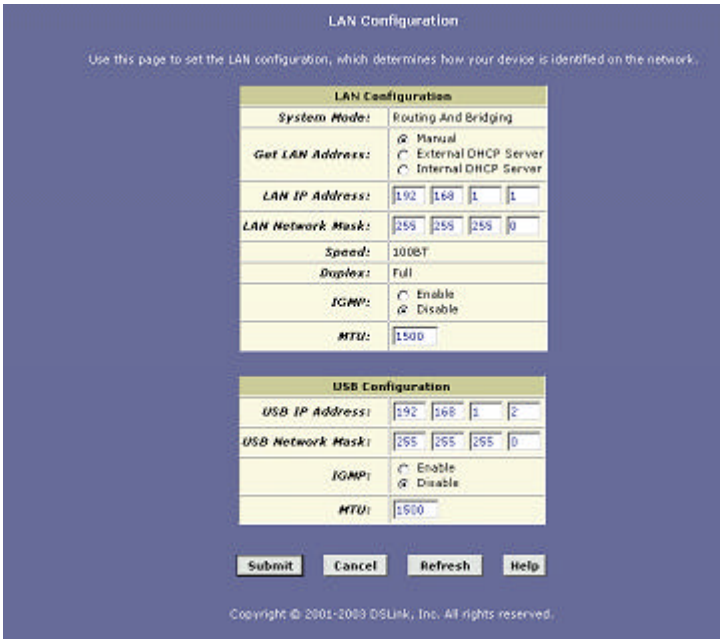


d. Certifique-se de que **Enable** esteja selecionado para o item **Bridging** e clique em **Submit**. A página de confirmação é exibida para confirmar suas alterações.

4. Configuração da LAN.

a. Selecione **Bridging** > **LAN Config**.

b. Não modifique as definições; basta manter o padrão mostrado conforme a figura abaixo:

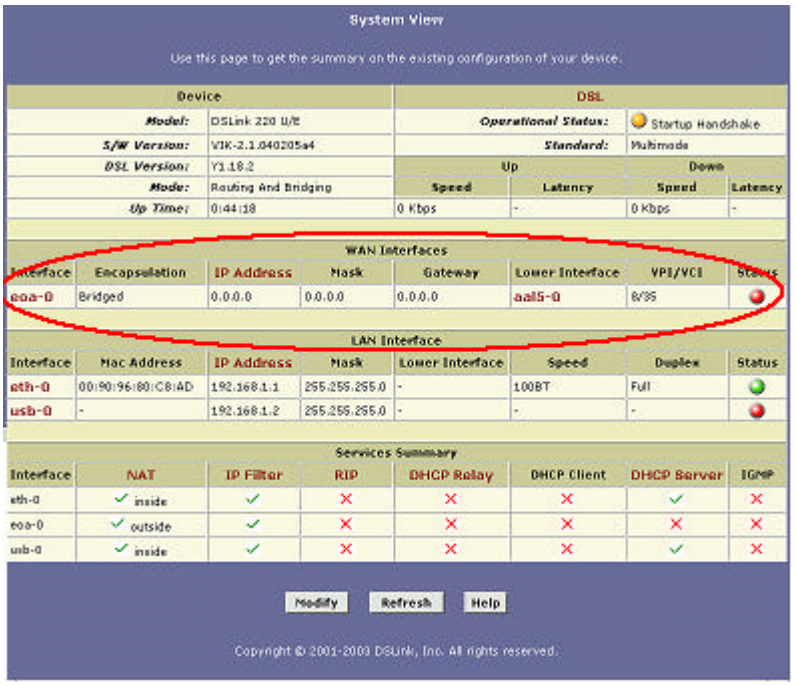


5. Efetive suas alterações.

Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

Parte 2: Verifique o status de sua conexão.

O item Interface WAN deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.


System View
Use this page to get the summary on the existing configuration of your device.
Device
Model: DSLink 220 U/E
S/W Version: VIK-2.1.040205s4
DSL Version: Y1.18.2
Mode: Routing And Bridging
Up Time: 0:44:18
DSL
Operational Status: Startup Handshake
Standard: Multimode
Up
Speed: 0 Kbps
Latency: -
Down
Speed: 0 Kbps
Latency: -
WAN Interfaces
Interface | Encapsulation | IP Address | Mask | Gateway | Lower Interface | VPI/VCI | Status
eoa-0 | Bridged | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | aal5-0 | 8/35
LAN Interface
Interface | Mac Address | IP Address | Mask | Lower Interface | Speed | Duplex | Status
eth-0 | 00:90:96:80:C8:AD | 192.168.1.1 | 255.255.255.0 | - | 100BT | Full
usb-0 | - | 192.168.1.2 | 255.255.255.0 | - | - | -
Services Summary
Interface | NAT | IP Filter | RIP | DHCP Relay | DHCP Client | DHCP Server | IGMP
eth-0 | inside | | | | | |
eoa-0 | outside | | | | | |
usb-0 | inside | | | | | |
Modify
Refresh
Help
Copyright © 2001-2003 DSLink, Inc. All rights reserved.

Parte 3: Configurando o PC.

Opção 1: Seu PC utiliza o IP fornecido por seu ISP.

Se este for o caso, configure seu PC para utilizar o IP estático fornecido por seu ISP, por exemplo:

IP address: 10.100.16.2

Subnet mask: 255.255.255.0

Default gateway: 10.100.16.254

Nota

Com a configuração acima, seu PC deve ser capaz de acessar a Internet agora, mas perderá a conexão local com a porta LAN do dispositivo. Se quiser configurar o DSLink 220 por meio do Navegador da Web novamente, deverá ser reconfigurado o PC para **192.168.1.x** para estar na mesma sub-rede da porta LAN do dispositivo.

Opção 2: Seu cliente utiliza o software PPPoE para conectar-se a seu ISP.

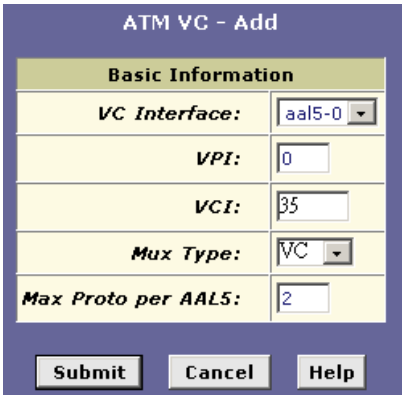
Basta manter a definição de seu PC como cliente DHCP e executar o software PPPoE para fazer a conexão.

Modo PPP Connection

Parte 1: Configurando o DSLink 220

1. Criando uma interface ATM VCC.

a. Selecione **Routing**> **ATM VC** > **Add** para visualizar a página ATM VC-Add.



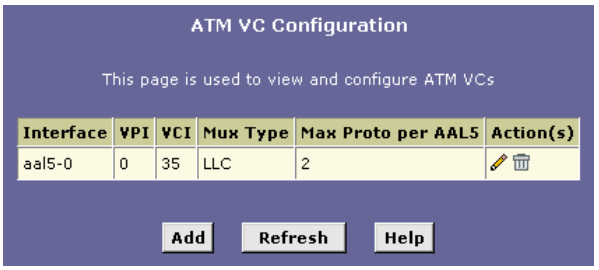
b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
VCC Interface	Selecione a interface VCC entre as interfaces disponíveis, p.ex., ***aal5-0***.
VPI/VCI	Insira os valores VPI/VCI fornecidos por seu ISP, p.ex., **0/35**.
Mux Type	Selecione **LLC** ou **VC**, conforme solicitado pelo seu ISP.
Max Proto per AAL5	Mantenha o padrão.

Após digitar os campos acima, clique **Submit**.

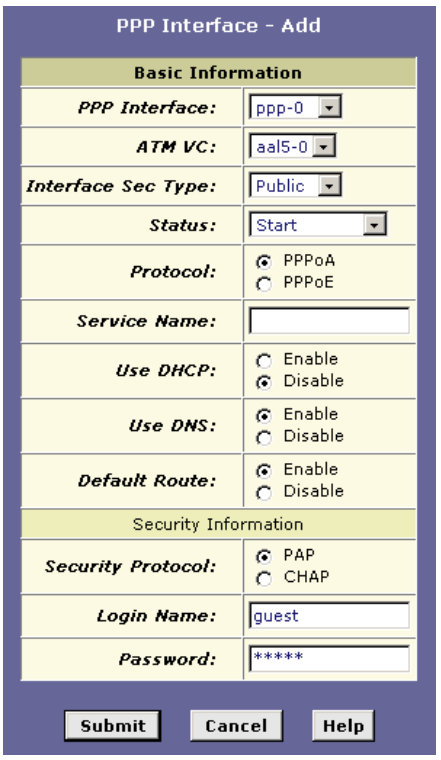
c. Quando aparecer a página de confirmação, clique em **Close**.

d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VCC recém-adicionada.



2. Criando a interface PPP.

a. Selecione **Routing** > **PPP** > **Add** para adicionar uma nova interface PPP.



b. Digite os campos fornecidos conforme abaixo.

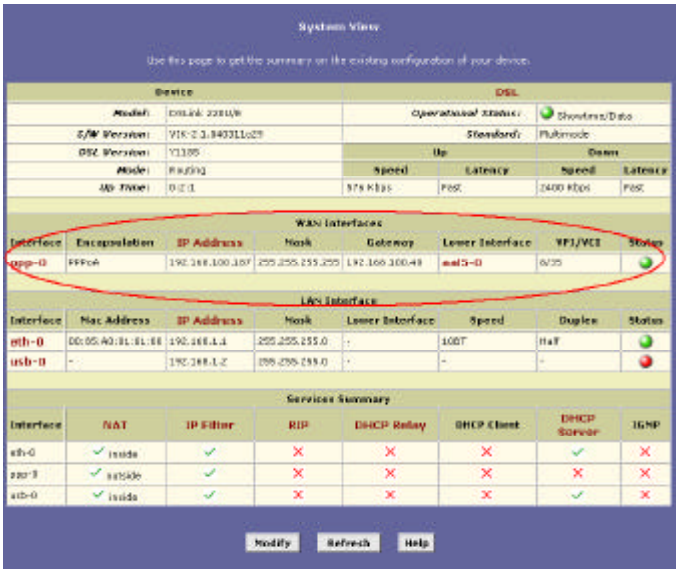
Campo	Descrição
PPP Interface	Selecione a interface PPP entre as interfaces disponíveis, p.ex., ***ppp-0***.
ATM VCC	Selecione o ATM VCC que foi criada no passo 1, p.ex., ***aal5-0***.
Interface Sec Type	**Public**
Status	Selecione **Start** ou **StartOnData**. **Start** – Para estabelecer conexão sempre que for ligado o DSLink 220. **StartOnData** – Para estabelecer conexão sempre que o dispositivo obtiver requisição para conectar-se à Internet, como quando é aberto um navegador requisitando páginas da Web.
Protocol	**PPPoA** ou **PPPoE** conforme exigido por seu ISP.
Service Name	Para **PPPoA**, não há necessidade de configuração. Para **PPPoE**, digite o Nome do Serviço se este for requisitado por seu ISP. Do contrário, deixe em

Campo	Descrição
	branco.
Use Dhcp	Selecione **Disable** a menos que seu ISP o instrua a ativar este serviço.
Use DNS	**Enable**
Default Route	**Enable**
Security Protocol	Selecione **PAP** ou **CHAP** conforme exigido por seu ISP.
Login Name	O nome de login fornecido por seu ISP.
Password	A senha fornecida por seu ISP.

c. Então retornará à página PPP Configuration e verá a nova interface PPP. **Oper. Status Link Up** indica que o link está atualmente ativo.

Parte 2: Verifique o status de sua conexão.

O item WAN Interface deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.



Parte 3: Configurando o PC.

Mantenha a configuração de seu PC como cliente DHCP. Nenhuma configuração adicional é necessária.

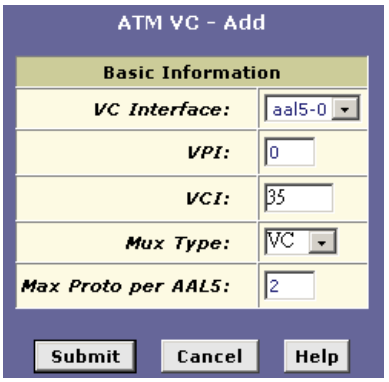
Modo Router Connection

Esta seção descreve os métodos de conexão por Router **RFC1577** e **RFC1483**

Parte 1: Configurando o DSLink 220

1. Criando uma interface ATM VCC.

a. Selecione **WAN** > **ATM VC** > **Add** para adicionar uma nova interface ATM VCC.



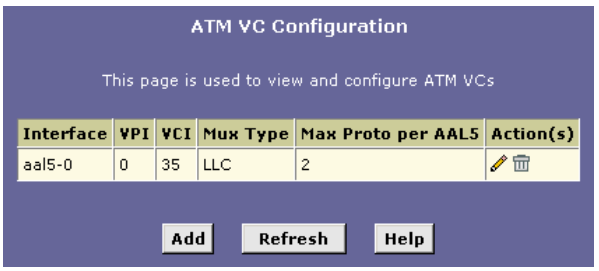
b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
VCC Interface	Selecione uma interface VCC entre as interfaces disponíveis, p.ex., ***aal5-0***.
VPI/VCI	Digite os valores VPI/VCI fornecidos por seu ISP, p.ex., **0/35**.
Mux Type	Selecione **LLC** ou **VC** conforme exigido por seu ISP.
Max Proto per AAL5	Mantenha o padrão.

Após digitar os campos acima, clique em **Submit**.

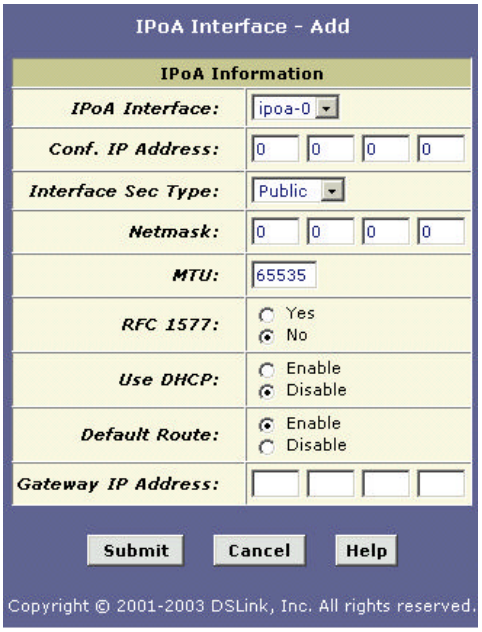
c. Quando aparecer a página de confirmação, clique em **Close**.

d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VC recém-adicionada.



2. Criando uma interface IPoA.

a. Selecione **WAN** > **IPoA** > **Add** para adicionar uma nova interface IPoA.



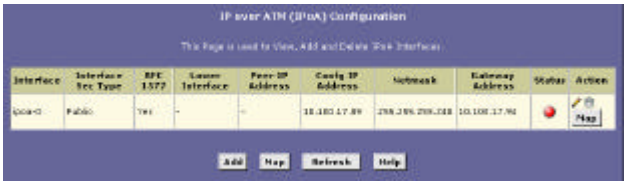
b. Então entre os campos abaixo.

Campo	Descrição
IPoA Interface	Selecione uma interface IPoA entre as interfaces disponíveis, p.ex., ***ipoa-0***.
Conf. IP Address	Digite o endereço IP fornecido por seu ISP, p.ex., **10.100.17.89**.
Interface Sec Type	**Public**
Net Mask	Digite o endereço IP fornecido por seu ISP, p.ex., **255.255.255.248**.
IPoA Type	Para RFC 1577-IP Clássico e ARP sobre ATM, selecione **Yes**. Para RFC 1483 Router, selecione **No**.
Default Route	**Enable**
Gateway IP Address	Digite o endereço IP fornecido por seu ISP, p.ex., **10.100.17.94**.

Após digitar os campos acima, clique em **Submit**.

c. Quando aparecer a página de confirmação, clique em **Close**.

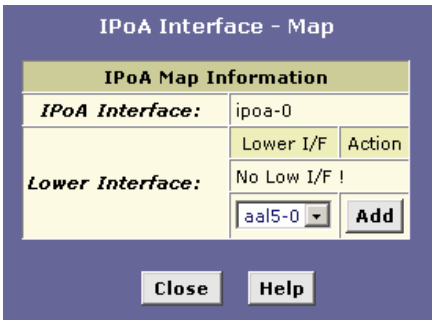
d. Então retornará à tabela **IPoA Configuration** e verá a entrada IPoA recém-adicionada.



3. Mapeando a interface IPoA em uma inteface baixa.

Na tabela **IPoA Configuration**, localize a nova entrada IPoA e clique em **Map** na coluna **Action**.

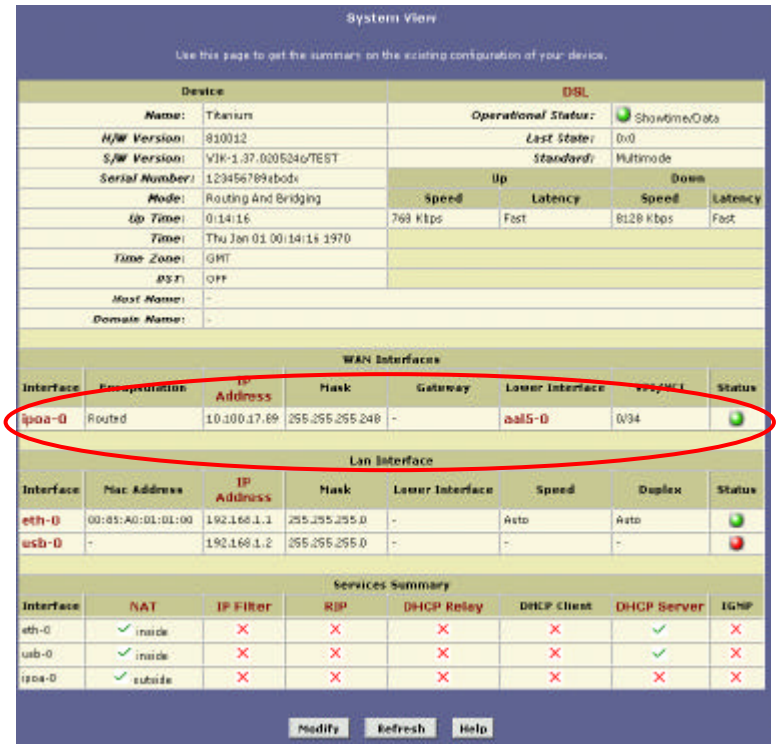
Na página **IPoA Interface-Map**, da lista drop-down, selecione o ATM VC que você criou no passo 1 para ser mapeada nesta interface IPoA e então clique em **Add**. Então clique em **Close** para sair da página de confirmação.



Você retornará para a página **IPoA Configuration** e verá que a interface baixa foi mapeada nesta interface IPoA.

Parte 2: Verifique o status de sua conexão.

O item WAN Interface deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.



Parte 3: Configurando o PC.

Mantenha a configuração de seu PC como cliente DHCP. Nenhuma configuração adicional é necessária.

7 Configurando Rotas IP

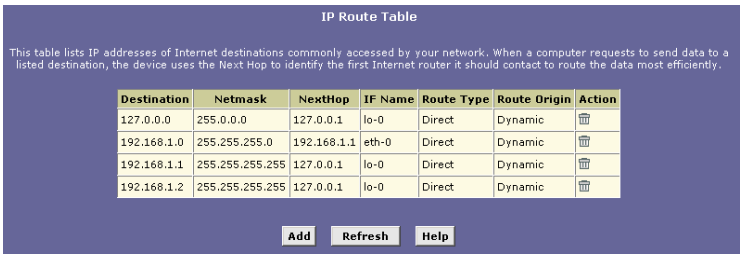
Você pode usar o Configuration Manager para definir rotas específicas para seus dados de Internet e de rede. Este capítulo fornece instruções para a criação de rotas.

A maioria dos usuários não precisa definir rotas IP. Poderá ser preciso definir rotas se:

- A instalação de sua rede incluir duas ou mais redes ou sub-redes.
- For conectar-se a dois ou mais serviços de ISP.
- For conectar-se a uma LAN corporativa remota.

Visualizando a Tabela de Roteamento IP

Para visualizar a tabela de roteamento do DSLink 220, selecione **Routing** > **IP Route**. É exibida a página a seguir:

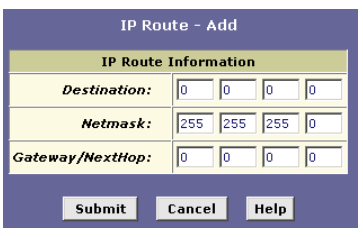

IP Route Table
This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.
Destination Netmask NextHop IF Name Route Type Route Origin Action
127.0.0.0 255.0.0.0 127.0.0.1 lo-0 Direct Dynamic
192.168.1.0 255.255.255.0 192.168.1.1 eth-0 Direct Dynamic
192.168.1.1 255.255.255.255 127.0.0.1 lo-0 Direct Dynamic
192.168.1.2 255.255.255.255 127.0.0.1 lo-0 Direct Dynamic
Add
Refresh
Help

A página IP Route Table inclui rotas que foram predefinidas no dispositivo, rotas podem ter sido adicionadas e rotas que o dispositivo tenha identificado automaticamente através de comunicação com outros dispositivos.

A tabela de roteamento deve refletir um gateway padrão, que direcione o tráfego Internet de saída para seu ISP. Este gateway padrão está mostrado na linha que contém o endereço de destino 0.0.0.0.

Adicionando Rotas IP

1. Selecione **Routing** > **IP Route** > **Add**. É exibida a página IP Rota – Add:



2. Especifique o destino, a máscara da rede e o gateway ou o próximo salto desta rota.

Para criar uma rota que defina o gateway padrão de sua LAN, digite **0.0.0.0** nos campos **Destination** e **Net Mask**. Digite o endereço IP de seu ISP no campo **Gateway**/**NextHop**.

Não é possível especificar um nome de interface, tipo de rota ou origem da rota. Estes parâmetros são utilizados apenas para rotas que são identificadas automaticamente à medida que o dispositivo se comunica com outros dispositivos de roteamento. Para as rotas que forem criadas, a tabela de roteamento exibe os valores padrão do sistema nestes campos.

3. Clique em **Submit**.

   A Tabela de Roteamento IP agora exibirá a nova rota.

4. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

8 Configuração DHCP

É possível configurar sua rede e o DSLink 220 para usar o Dynamic Host Configuration Protocol (DHCP). Este capítulo fornece instruções para a implementação do DHCP em sua rede.

Modos DSLink 220 DHCP

O dispositivo pode ser configurado como um servidor DHCP, agente de retransmissão DHCP ou, em alguns casos, um cliente DHCP.

- **DHCP Server -** Ele manterá o pool de endereços e os distribuirá para seus computadores da LAN. Se o pool de endereços incluir endereços IP privados, então deverá também configurar o serviço Conversão de Endereços de Rede, para que os endereços privados possam ser convertidos para seu endereço IP público na Internet. Tanto o servidor DHCP quanto o NAT estão ativados na configuração padrão.
- **DHCP relay agent** - Se seu ISP executa a função de servidor DCHP para sua rede, então poderá configurar o dispositivo como agente de retransmissão DHCP. Quando o DSLink 220 recebe uma requisição para acesso à Internet a partir de um computador de sua rede, ele contata seu ISP para as informações de IP necessárias e, em seguida, retransmite as informações partilhadas de volta ao computador.
- **DCHP Client -** Caso tenha outro PC ou dispositivo em sua rede que já esteja executando a função de servidor DHCP, poderá configurar a porta LAN do DSLink 220 para ser um cliente DHCP daquele servidor.

Configurando o Servidor DHCP

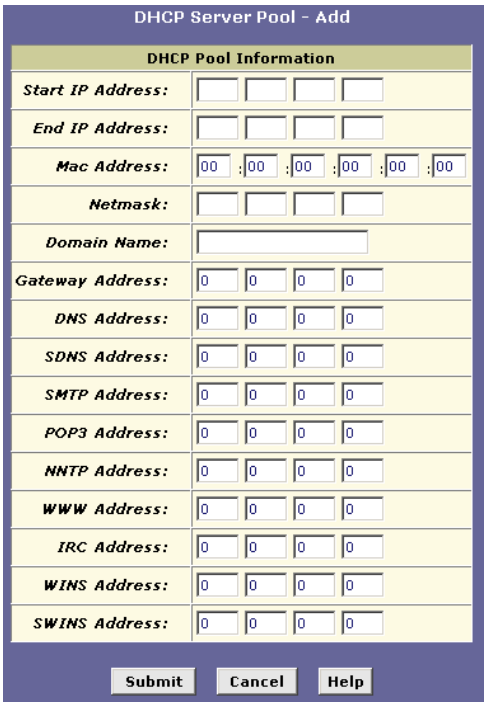
Parte 1. Criando pools de endereços IP

1. Selecione **LAN** > **DHCP Server**. É exibida a página DHCP Server Configuration:

Cada pool que for criado exibe uma linha na tabela sobre esta página. É possível criar até oito pools. Neste exemplo, foi criado um pool para a interface LAN e outro para a interface USB. Pools adicionais podem ser necessários quando o dispositivo for configurado com várias interfaces LAN.

2. Para adicionar um pool de endereços IP, clique em **Add**.

   É exibida a página DHCP Server Pool – Add.



Os campos ***Start IP Address***, ***End IP Address***, ***Net Mask***, e ***Gateway Address*** são obrigatórios; os outros são opcionais.

Campo	Descrição
Start/End IP Addresses	Especifique os endereços primário e secundário do pool.
Mac Address	Permite atribuir endereço IP específico a um computador específico, identificado por este endereço MAC. Se este for o caso, então deve ter especificado o mesmo endereço IP nos campos Start/End IP Address.
Net Mask	Especifica a máscara de sub-rede associada do endereço IP nesta faixa.
Domain Name	O nome de domínio a ser utilizado por clientes DHCP.
Gateway Address	O endereço do gateway padrão. Normalmente, ele é o endereço IP da porta LAN do dispositivo.
DNS	O endereço IP do servidor DNS. Normalmente ele é encontrado em seu ISP.
SDSN...SWINS (opcional)	Os endereços IP dos dispositivos que executam variados serviços para clientes DHCP.

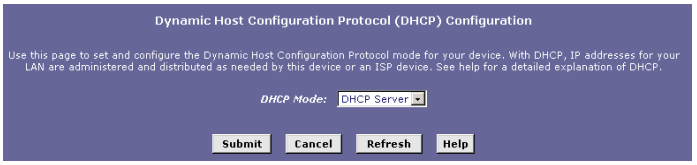
3. Clique em **Submit**.

   É exibida a página de confirmação para indicar que o pool foi adicionado com sucesso.

4. Clique em **Close** para retornar à página DHCP Configuration.

Parte 2. Ativando o Modo DHCP Server

1. Selecione **LAN** > **DHCP Mode**, na lista suspensa DHCP Mode, selecione **DHCP Server** e, em seguida, clique em **Submit**.


Dynamic Host Configuration Protocol (DHCP) Configuration
Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.
DHCP Mode:
DHCP Server
Submit
Cancel
Refresh
Help

   É exibida uma página para confirmar a alteração.

2. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Parte 3. Configurando seus PCs como clientes DHCP

Para cada computador que queira configurar para receber informações de IP automaticamente, configure as propriedades de TCP/IP para "Obtain an IP address automatically" (o texto real poderá variar dependendo de seu sistema operacional).

Modificando Pools de Endereços

Selecione **LAN** > **DHCP Server** e, em seguida, clique no ícone Modify no pool DHCP que quiser modificar. É exibida a página DHCP Server Pool – Modify:

Ao modificar um pool de endereços, terá permissão ***apenas*** para:

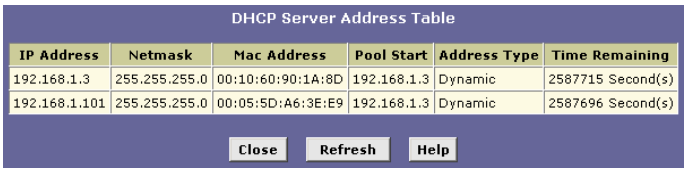
- Alterar o nome de domínio associado ao pool.
- Excluir da distribuição endereços IP dentro de sua faixa. Para excluir um endereço IP, digite-o nos campos fornecidos e clique em **Add**.

Se quiser alterar outros atributos, será preciso excluir o pool e criar um novo.

Após digitar suas alterações, clique em **Submit** e certifique-se de utilizar o recurso Commit para salvar suas alterações na memória permanente.

Visualizando Atribuições de Endereço DHCP Atuais

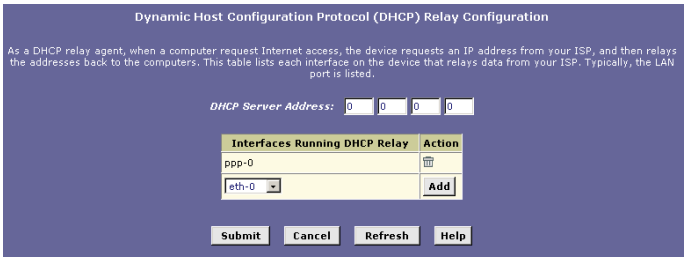
Para visualizar uma tabela de todas as atribuições de endereço IP atuais, selecione **LAN** > **DHCP Server** > **Address Table**. A página DHCP Server Address Table é a seguinte:



Configurando a Retransmissão DHCP

Parte 1. Definindo a(s) interface(s) de retransmissão DHCP

1. Selecione **LAN** > **DHCP Relay**. É exibida a página DHCP Relay Configuration:


Dynamic Host Configuration Protocol (DHCP) Relay Configuration
As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.
DHCP Server Address:
0
0
0
0
Interfaces Running DHCP Relay
Action
ppp-0
eth-0
Add
Submit
Cancel
Refresh
Help

   Esta página oferece uma caixa de texto para a digitação do endereço IP do servidor DHCP de seu ISP e uma tabela que apresenta uma lista das interfaces existentes em seu DSLink 220 que possam retransmitir Informações sobre DHCP.

2. Digite o endereço IP do servidor DHCP de seu ISP nos campos fornecidos.

   Se não possuir este número, não será necessário inseri-lo aqui. Requisições para informações de IP provenientes de sua LAN serão transferidas para o gateway padrão, que deve rotear a requisição da forma apropriada.

3. Se a interface identificada como eth-0 já não estiver sendo exibida, selecione-a na lista suspensa e clique em **Add.**

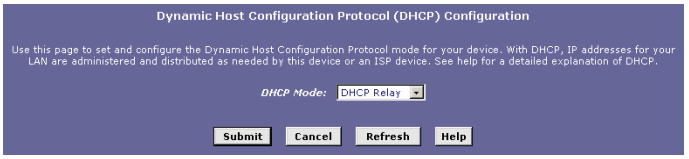
4. Clique em **Submit**.

   É exibida uma página para confirmar suas alterações.

Parte 2. Ativando modo de retransmissão DHCP

1. Selecione **LAN** > **DHCP Mode**, na lista suspensa DHCP Mode, selecione **DHCP Relay** e, em seguida, clique em **Submit**.

   É exibida uma página para confirmar a alteração.


Dynamic Host Configuration Protocol (DHCP) Configuration
Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.
DHCP Mode:
DHCP Relay
Submit
Cancel
Refresh
Help

2. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Parte 3. Configurando seus PCs como clientes DHCP

Para cada computador que queira configurar para receber informações de IP automaticamente, configure as propriedades de TCP/IP para "Obtain an IP address automatically" (o texto real poderá variar dependendo de seu sistema operacional).

9 Configuração NAT

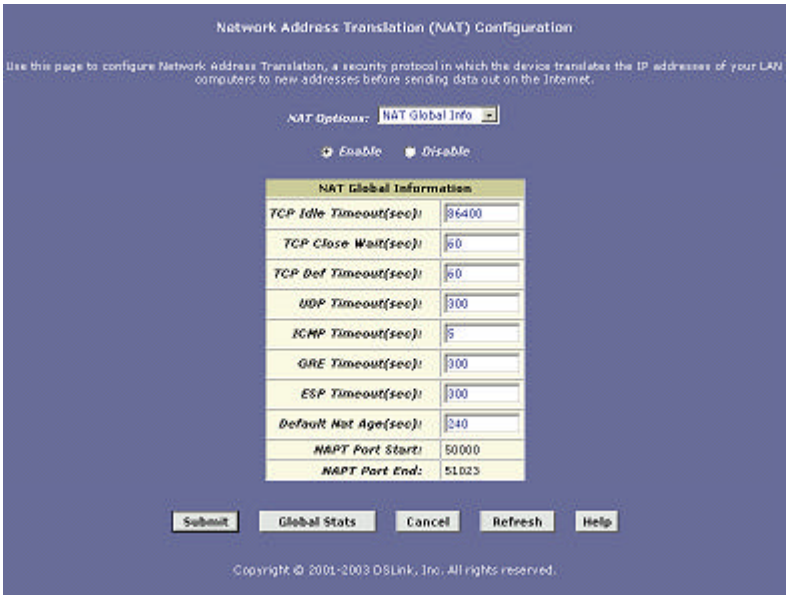
Este capítulo fornece uma visão geral da Conversão de Endereços de Rede (NAT, network address translation) e instruções para modificar a configuração padrão em seu dispositivo.

Sua Instalação NAT Padrão

Por padrão, a NAT é ativada, com uma regra *network address port translation* (napt) configurada que converte qualquer endereço privado no lado LAN no endereço IP público atribuído por seu ISP no lado WAN.

Visualizando Sua Configuração NAT

Para visualizar suas configurações NAT, selecione **Services** > **NAT**. É exibida a página NAT Configuration:



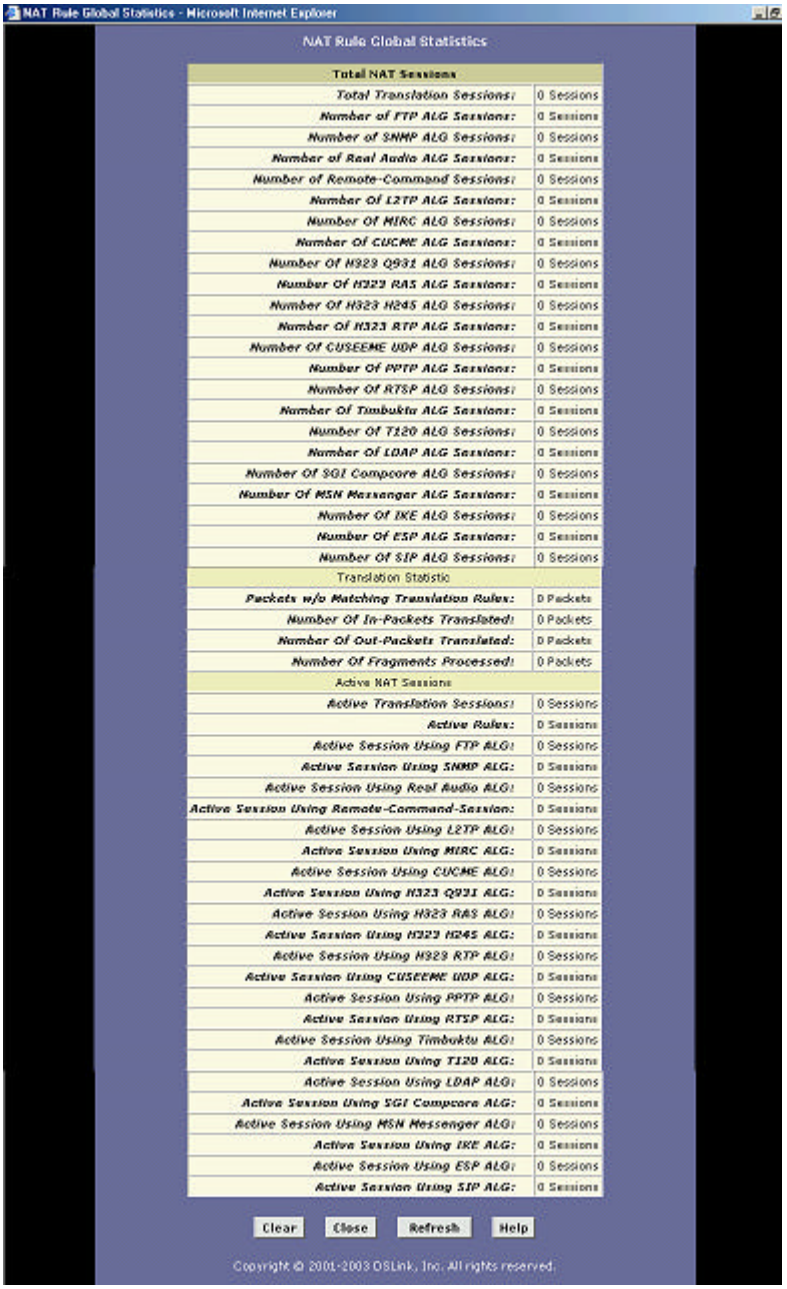
A tabela NAT Global Information contém os seguintes campos:

Campo	Descrição
TCP Idle Timeout (seg)	Para a sessão de conversão NAT sobre dados que utilizem o protocolo TCP, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido após decorrido o tempo especificado.
TCP Close Wait (seg)	Para a conversão NAT sobre dados usando o protocolo TCP, após a sessão de comunicação ter sido encerrada, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido

Campo	Descrição
	após decorrido o tempo especificado.
TCP Def Timeout (seg)	Para a sessão de conversão NAT sobre dados que utilizem o protocolo TCP, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido após decorrido o tempo especificado.
UDP Timeout (seg)	O mesmo que TCP Idle Timeout, mas para pacotes UDP.
ICMP Timeout (seg)	O mesmo que TCP Idle Timeout, mas para pacotes ICMP.
GRE Timeout (seg)	O mesmo que TCP Idle Timeout, mas para pacotes GRE.
Default Nat Age (seg)	Para todas as outras sessões de conversão NAT, o número de segundos após o qual uma sessão de conversão não mais será válida.
NAPT Port Start/End	Quando uma regra napt é definida, as portas de origem serão convertidas para números seqüenciais nesta faixa.

Se você alterar algum valor, clique em **Submit** e, em seguida, efetive suas alterações armazenando-as na memória permanente do sistema.

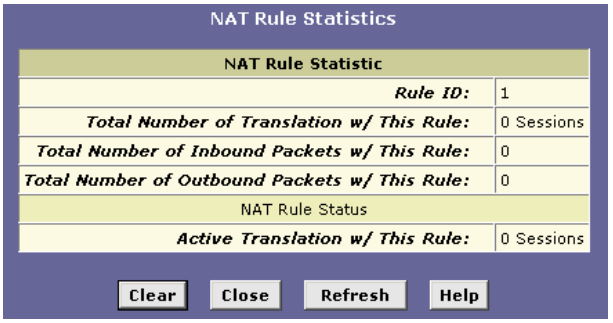
Então pode clicar em **Global Stats** para visualizar dados acumulados sobre quantas regras NAT foram chamadas e quantos dados foram convertidos. É exibida uma página similar à abaixo:


NAT Rule Global Statistics - Microsoft Internet Explorer
NAT Rule Global Statistics
Total NAT Sessions
Total Translation Sessions: 0 Sessions
Number of FTP ALG Sessions: 0 Sessions
Number of SNMP ALG Sessions: 0 Sessions
Number of Real Audio ALG Sessions: 0 Sessions
Number of Remote-Command Sessions: 0 Sessions
Number Of L2TP ALG Sessions: 0 Sessions
Number Of MIRC ALG Sessions: 0 Sessions
Number Of CUCME ALG Sessions: 0 Sessions
Number Of H323 Q931 ALG Sessions: 0 Sessions
Number Of H323 RAS ALG Sessions: 0 Sessions
Number Of H323 H245 ALG Sessions: 0 Sessions
Number Of H323 RTP ALG Sessions: 0 Sessions
Number Of CUSEEME UDP ALG Sessions: 0 Sessions
Number Of PPTP ALG Sessions: 0 Sessions
Number Of RTSP ALG Sessions: 0 Sessions
Number Of Timbukta ALG Sessions: 0 Sessions
Number Of T120 ALG Sessions: 0 Sessions
Number Of LDAP ALG Sessions: 0 Sessions
Number Of SGI Compcore ALG Sessions: 0 Sessions
Number Of MSN Messenger ALG Sessions: 0 Sessions
Number Of IKE ALG Sessions: 0 Sessions
Number Of ESP ALG Sessions: 0 Sessions
Number Of SIP ALG Sessions: 0 Sessions
Translation Statistic
Packets w/o Matching Translation Rules: 0 Packets
Number Of In-Packets Translated: 0 Packets
Number Of Out-Packets Translated: 0 Packets
Number Of Fragments Processed: 0 Packets
Active NAT Sessions
Active Translation Sessions: 0 Sessions
Active Rules: 0 Sessions
Active Session Using FTP ALG: 0 Sessions
Active Session Using SNMP ALG: 0 Sessions
Active Session Using Real Audio ALG: 0 Sessions
Active Session Using Remote-Command-Session: 0 Sessions
Active Session Using L2TP ALG: 0 Sessions
Active Session Using MIRC ALG: 0 Sessions
Active Session Using CUCME ALG: 0 Sessions
Active Session Using H323 Q931 ALG: 0 Sessions
Active Session Using H323 RAS ALG: 0 Sessions
Active Session Using H323 H245 ALG: 0 Sessions
Active Session Using H323 RTP ALG: 0 Sessions
Active Session Using CUSEEME UDP ALG: 0 Sessions
Active Session Using PPTP ALG: 0 Sessions
Active Session Using RTSP ALG: 0 Sessions
Active Session Using Timbuktu ALG: 0 Sessions
Active Session Using T120 ALG: 0 Sessions
Active Session Using LDAP ALG: 0 Sessions
Active Session Using SGI Compcore ALG: 0 Sessions
Active Session Using MSN Messenger ALG: 0 Sessions
Active Session Using IKE ALG: 0 Sessions
Active Session Using ESP ALG: 0 Sessions
Active Session Using SIP ALG: 0 Sessions
Clear
Close
Refresh
Help
Copyright © 2001-2003 DSLink, Inc. All rights reserved.

Visualizando Regras NAT e Estatísticas de Regras

Para visualizar as Regras NAT atualmente definidas em seu sistema, selecione **Services** > **NAT** > **NAT Rule Entry**. É exibida a página NAT Rule Configuration:

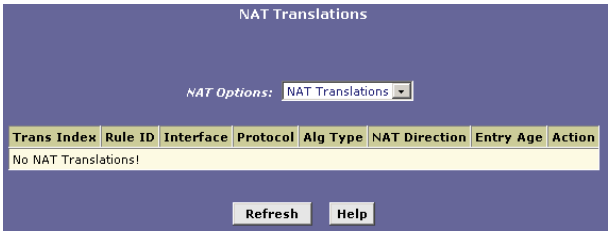
Para visualizar dados sobre a freqüência com que uma regra NAT específica foi utilizada, clique em **Stats**. É exibida uma página similar à abaixo:


NAT Rule Statistics
NAT Rule Statistic
Rule ID: 1
Total Number of Translation w/ This Rule: 0 Sessions
Total Number of Inbound Packets w/ This Rule: 0
Total Number of Outbound Packets w/ This Rule: 0
NAT Rule Status
Active Translation w/ This Rule: 0 Sessions
Clear
Close
Refresh
Help

As estatísticas mostram quantas vezes esta regra foi chamada e quantas sessões atualmente ativas estão utilizando esta regra.

Visualizando Conversões NAT Atuais

Para visualizar uma lista de conversões NAT que tenham recentemente sido executadas e que permaneçam em vigor (para qualquer uma das regras definidas), selecione **Services** > **NAT** > **NAT Translations**. É exibida a página NAT Translations:



Para cada sessão de conversão atual NAT, a tabela contém os seguintes campos:

Campo	Descrição
Trans Index	O número seqüencial atribuído à sessão IP utilizado por esta sessão de conversão NAT.
Rule ID	A identificação da regra NAT chamada.
Interface	A interface do dispositivo sobre o qual a regra NAT foi chamada (a partir da definição da regra).
Protocol	O protocolo IP utilizado pelos pacotes de dados que estiverem sofrendo conversões (a partir da definição da regra) Exemplo: TCP,

Campo	Descrição
	UDP, ICMP.
Alg Type	O *Application Level Gateway* (ALG), se houver, que foi utilizado para ativar esta conversão NAT (ALGs são configurações especiais que determinados aplicativos exigem para funcionar enquanto a NAT estiver ativada).
NAT Direction	A direção (de entrada ou de saída) da conversão (a partir da definição da porta).
Entry Age	O tempo decorrido, em segundos, da sessão de conversão NAT.

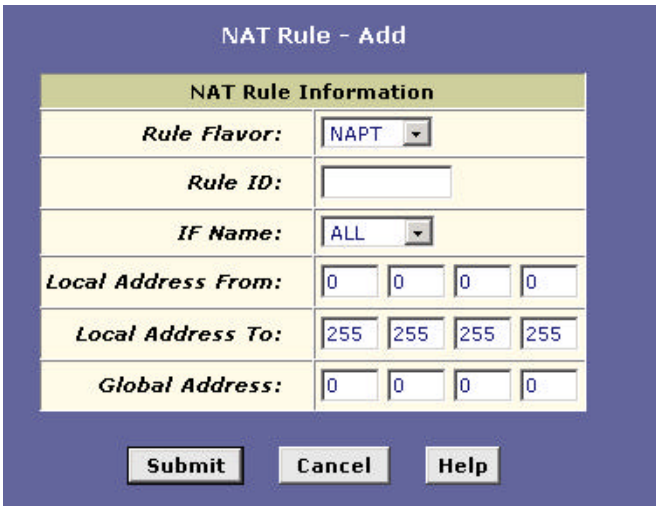
Adicionando Regras NAT

Esta seção explica como criar regras para as diferentes versões NAT.

A regra napt: Efetuando conversões entre endereços IP públicos e privados

A versão NAT napt foi utilizada em sua configuração padrão. A versão napt converte todos os endereços IP de origem privados do lado LAN em um único endereço IP público. Ela também converte os números da porta de origem em números de porta que são definidos na página NAT Global Configuration.

1. Selecione **Services** > **NAT** > **NAT Rule Entry**> **Add**.



2. Clique na lista suspensa Rule ID para atribuir um número a uma regra.

   Rule ID determina a ordem na qual as regras são chamadas (a regra de número mais baixo é chamada primeiro, e assim por diante). Em alguns casos, duas ou mais regras podem ser definidas para agir sobre o mesmo conjunto de endereços IP. Assim que um pacote de dados corresponder a uma regra, os dados passarão a agir conforme essa regra e não ficarão sujeitos a regras de número mais alto.

3. Na Lista suspensa Rule Flavor, selecione **NAPT**, se necessário.

4. Na lista suspensa IFName, selecione a interface do DSLink 220 à qual esta regra se aplica.

   Normalmente, as regras NAT aplicam-se à comunicação entre sua LAN e a Internet. Como o dispositivo utiliza a interface WAN (identificada como *ppp-0* ou *eoa-0*) para conectar sua LAN a seu ISP, esta será a seleção usual de IFName.

5. Selecione um protocolo ao qual esta regra se aplique, ou escolha **ALL** se a regra aplicar-se a todos os dados.

6. Nos campos **Local Address From/To**, digite os endereços IP inicial e final, respectivamente, da faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos para especificar um único valor.

   Se todos os endereços LAN precisarem ser convertidos, especifique 0.0.0.0 e 255.255.255.255, respectivamente.

   Se for utilizar endereços privados não-seqüenciais, é possível criar uma regra napt adicional para cada faixa de endereços em separado.

7. No campo Global Address, digite o endereço que deseja que sirva como o endereço publicamente conhecido para o computador da LAN.

8. Quando tiver acabado de inserir todas as informações, clique em **Submit**.

   É exibida uma página para confirmar a alteração.

9. Clique em **Close** para retornar à página NAT Configuration.

   A nova regra deve ser exibida na tabela NAT Rule.

10. Selecione **NAT Global Info** da lista **NAT Options** para ir para a página NAT Configuration. Certifique-se de que o botão **Enable** está ligado.

11. Na página NAT Configuration, clique em **Submit**.

    É exibida uma página para confirmar suas alterações.

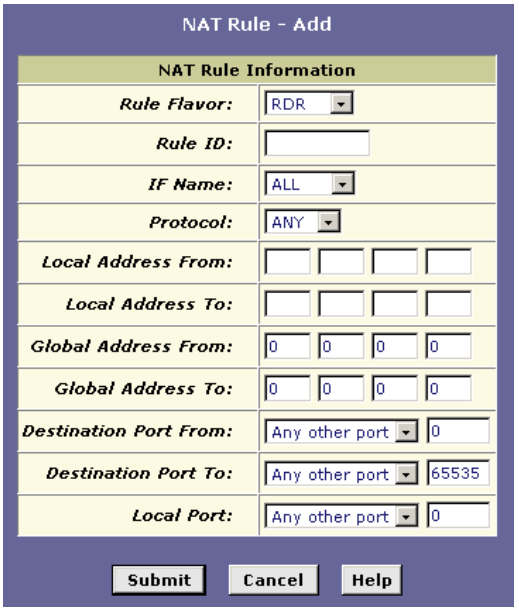
12. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

A regra rdr: Permitindo acesso externo a um computador da LAN

É possível criar uma regra rdr para fazer com que um computador de sua LAN, como um servidor Web ou FTP, fique disponível para usuários da Internet sem ter que obter um endereço IP público para esse computador. O endereço IP privado do computador é convertido para seu endereço IP público em todos os pacotes de dados de entrada e de saída.

Nota

Sem uma regra rdr (ou regra bitmap), o DSLink 220 bloqueia tentativas por computadores externos de acesso a seus computadores da LAN.



Siga estas instruções para adicionar uma regra rdr.

1. Exiba a página NAT Rule – Add, escolha um valor para Rule ID e selecione **RDR** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.

3. Nos campos **Local Address From**/**To**, digite o mesmo endereço IP privado ou os endereços primário e secundário em uma faixa:

   - Caso venha a digitar o mesmo endereço IP em ambos os campos, o tráfego de entrada que corresponder aos critérios desta regra será redirecionado àquele endereço IP.
   - Caso venha a digitar uma faixa de endereços, o tráfego de entrada será redirecionado a qualquer computador disponível naquela faixa. Esta opção normalmente seria utilizada para balanceamento de carga, por meio do qual o tráfego é distribuído entre diversos servidores redundantes.

4. Nos campos **Global Address From**/**To**, digite o endereço IP público que lhe foi atribuído por seu ISP.

   Caso tenha várias interfaces WAN, em ambos os campos digite o endereço IP da interface à qual esta regra se aplica. Esta regra não será posta em execução para dados que chegarem em interfaces WAN não especificadas aqui.

   Caso tenha várias interfaces WAN e quiser que a regra seja posta em execução em uma faixa delas, digite os endereços IP inicial e final da faixa.

5. Nos campos **Destination Port From**/**To**, entre ou selecione o ID da porta (ou uma faixa) que você espera encontrar nos pacotes que chegam, destinados aos computadores da LAN para os quais esta regra foi criada.

   O tráfego de entrada que obedece este critério será redirecionado para o número da porta local que você especificou no próximo passo.

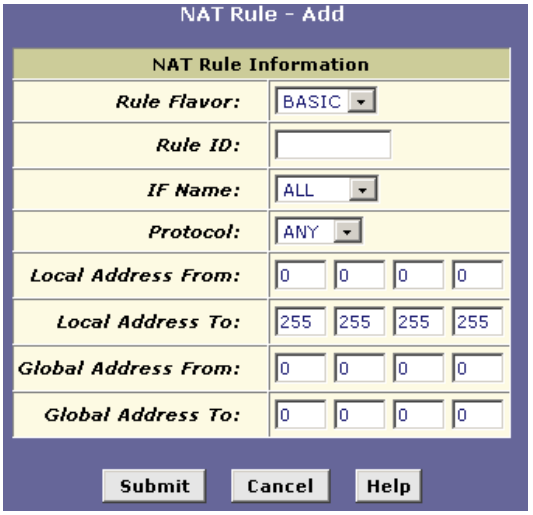
6. Se o computador da LAN que você está disponibilizando publicamente está configurado para usar um número de porta não padrão para o tipo de tráfego que ele recebe, digite um número de porta não padrão no campo **Local Port**.

7. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra basic: Executando conversões 1:1

A versão basic converte o endereço IP privado (lado LAN) em um endereço público (lado WAN), como regras napt. No entanto, ao contrário das regras napt, as regras basic não convertem também os números de porta no cabeçalho de pacote; eles são passados sem conversão. Portanto, a regra basic não proporciona o mesmo nível de segurança que a regra napt.

A figura abaixo mostra os campos utilizados para a adição de uma regra basic.



1. Exiba a página NAT Rule – Add, escolha uma Rule ID e selecione **BASIC** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.

3. Nos campos **Local Address From**/**To**, digite os endereços IP inicial e final que identificam a faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos.

   Caso especifique uma faixa, cada endereço será convertido em seqüência para um endereço correspondente em uma faixa de endereços globais (especificada no passo 4).

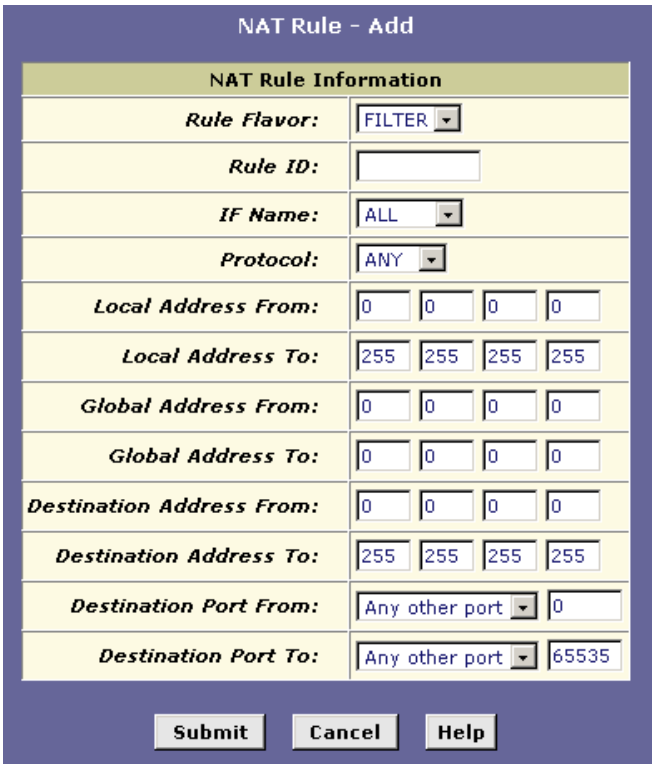
4. Nos campos **Global Address From**/**To**, digite o endereço inicial e final que identificam o pool de endereços IP públicos para o qual seus endereços privados devem ser convertidos. Ou digite o mesmo endereço em ambos os campos (caso também tenha sido especificado um único endereço no passo 3).

5. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra filter: Configurando uma regra basic com critérios adicionais

Da mesma forma que na versão basic, a versão filter converte endereços IP públicos e privados um a um. A versão filter amplia a capacidade da regra basic.

Então pode usar a regra filter se quiser que ocorra a conversão de um endereço somente quando seus computadores da LAN iniciarem o acesso a destinos específicos. Os destinos podem ser identificados por seus endereços IP, tipo de servidor (como servidor FTP ou Web) ou ambos.



1. Exiba a página NAT Rule – Add, escolha a Rule ID, e selecione **FILTER** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.

3. Nos campos **Local Address From**/**To**, digite os endereços IP inicial e final que identificam a faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos.

   Caso especifique uma faixa, cada endereço será convertido em seqüência para um endereço correspondente em uma faixa de endereços globais (especificada no passo 4).

4. Nos campos **Global Address From**/**To**, digite o endereço inicial e final que identificam a faixa de endereços IP públicos para a qual seus endereços privados devem ser convertidos. Ou digite o mesmo endereço em ambos os campos (caso também tenha sido especificado um único endereço no passo 3).

5. Especifique **Destination Address** ou **Destination Addresses**, **Destination Port** (ou **Destination Ports**), ou ambos. É possível especificar um único valor inserindo esse valor em ambos os campos.

   - Especifique um endereço de destino (ou faixa) caso queira que esta regra aplique-se apenas ao tráfego de saída até o endereço (ou faixa).

     Caso digite apenas a parte da identificação da rede do endereço de destino, a regra será aplicada ao tráfego de saída para todos os computadores na rede.

- Especifique uma porta de destino (ou faixa) caso queira que esta regra se aplique a qualquer tráfego de saída para os tipos de servidores identificados por esse número de porta.
- Especifique tanto um endereço de destino (ou faixa) quanto uma porta de destino (ou faixa) caso queira que esta regra de conversão seja aplicada aos acessos do tipo de servidor especificado no local especificado.

6. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

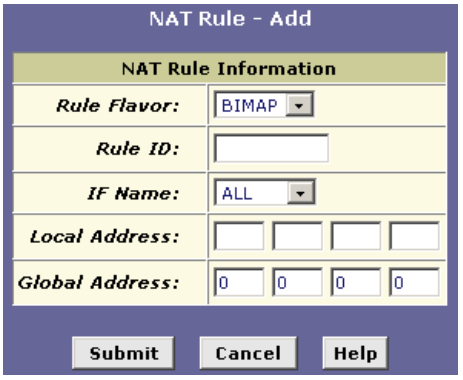
A regra bitmap: Executando conversões bidirecionais

Ao contrário das outras versões NAT, a versão bitmap executa conversões de endereço nas direções tanto de saída quanto de entrada.

Na direção de entrada, quando a interface especificada recebe um pacote destinado a seu endereço IP público, este endereço é convertido para o endereço IP privado de um computador em sua LAN.

Na direção de saída, o endereço IP de origem privado em um pacote de dados é convertido para o endereço IP público da LAN.

Regras bitmap podem ser utilizadas para proporcionar acesso externo a um dispositivo LAN. Elas não proporcionam o mesmo nível de segurança das regras rdr, pois as regras rdr também re-roteiam pacotes de entrada com base na identificação da porta. Regras bitmap não levam em conta o número de porta e, portanto, permitem acesso externo independentemente do tipo de porta de destino especificado no pacote de entrada.



1. Exiba a página NAT Rule – Add, escolha a Rule ID, e selecione **BITMAP** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.

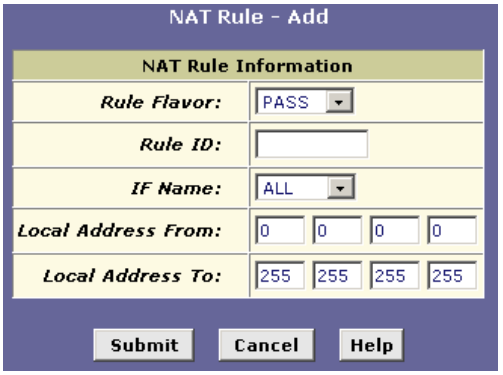
3. No campo Local Address, digite o endereço IP privado do computador ao qual esteja concedendo acesso externo.

4. No campo Global Address, digite o endereço que deseja que sirva como o endereço publicamente conhecido para o computador da LAN.

5. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra PASS : Permitindo que endereços específicos passem sem conversão

É possível criar uma regra PASS para permitir que uma faixa de endereços IP permaneça sem conversão quando outra regra a converteria.



Deve ser atribuída uma identificação de regra à regra PASS que seja um número inferior ao da identificação atribuída a uma regra que se pretenda transpor. Caso queira que um endereço IP específico ou faixa de endereços não fiquem sujeitos a uma regra existente, por exemplo, identificação de regra nº 5, será possível criar uma regra PASS com identificação nº 1a 4.

1. Exiba a página NAT Rule – Add Page, escolha a Rule ID, e selecione **Pass** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.

3. Nos campos **Local Address From** e **Local Address To** campos, digite os endereços primário e secundário IP que definem uma faixa de endereços privados que queira que passem sem conversão. Caso queira que uma regra PASS aja em apenas um endereço, digite esse endereço em ambos os campos.

4. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

10 Configurando Endereços do Servidor DNS e DDNS

Este capítulo descreve como configurar a função de retransmissão DNS e DDNS do DSLink 220.

Visão Geral da Retransmissão DNS

Ao executar a retransmissão DNS, o DSLink 220 propriamente dito não é um servidor DNS, ele transmite requisições DNS dos PCs da LAN para um servidor DNS no ISP. Em seguida, ele retransmite a resposta DNS aos PCs.

O DSLink 220 detecta o endereço DNS de uma ou ambas as maneiras a seguir:

- **Detectado através de PPP**
- **Configurado no DSLink 220**

Configurando a Retransmissão DNS

Siga estes passos para configurar a retransmissão DNS:

1. Configure os PCs da LAN.

   Basta definir os PCs da LAN como clientes DHCP do DSLink 220.

2. No DSLink 220, vá para **LAN** > **DHCP Server**, insira o endereço IP da LAN (p.ex., **192.168.1.1**) ou **0.0.0.0** como o endereço DNS no pool de servidores DHCP.

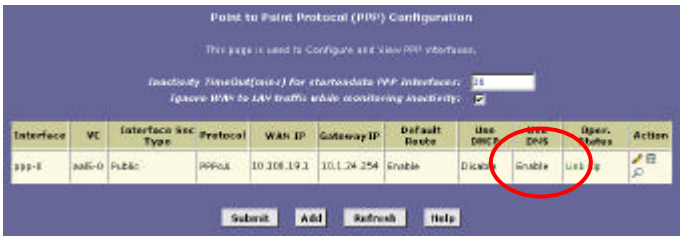
   Por padrão, 0.0.0.0 já é definido como o DNS do pool DHCP.

3. Determina de que forma o roteador detectará o endereço DNS do servidor:

   Opção 1: Usando a conexão PPP para detectar o DNS

   Use DNS deve ser ativado nas propriedades da interface PPP.

   Vá para **Routing** > **PPP** e verifique os detalhes da interface PPP. Se **Use DNS** estiver desativado, será preciso excluir a interface e criá-la novamente com a nova configuração.



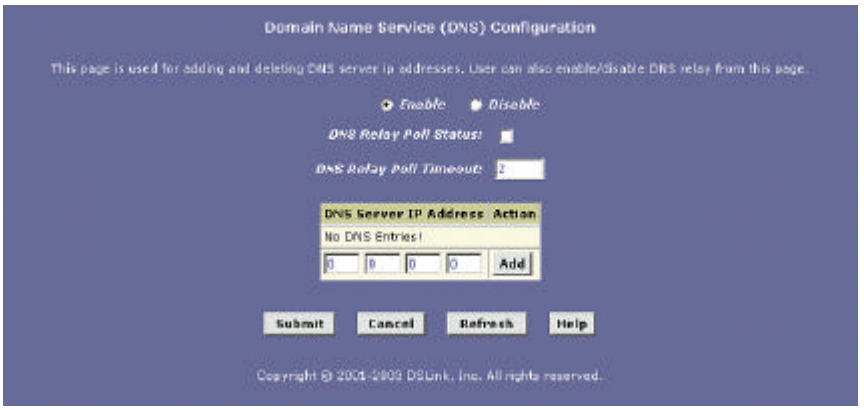
Opção 2: Configurando DNS no roteador ADSL/Ethernet

É possível configurar o endereço DNS do servidor para ser retransmitido sobre o roteador se uma das seguintes circunstâncias aplicar-se:

- Sem utilizar a conexão PPP para o ISP (ou se for utilizado um protocolo que não seja PPP, como o EoA).
- Então utiliza a conexão PPP e **Use DNS** já está **ativado**. Em seguida, esses endereços configurados serão utilizados além daqueles endereços DNS detectados através de PPP.
- Então utiliza a conexão PPP e **Use DNS** está **desativado**. Em seguida, esses endereços configurados serão utilizados.

Siga estes passos para configurar a retransmissão DNS no roteador:

(a) Vá para **Service** > **DNS** para exibir a página DNS Configuration.



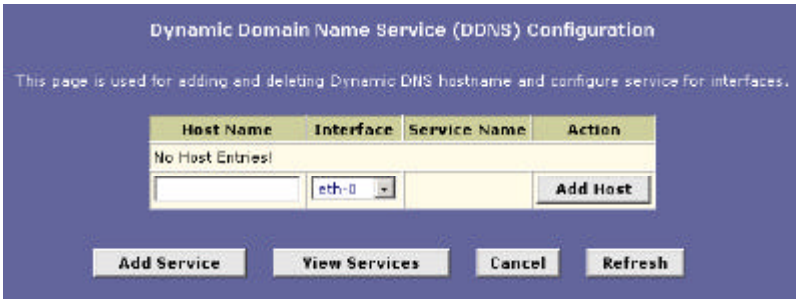
Página DNS Configuration

(b) Digite o endereço IP do servidor DNS em uma linha vazia e clique em **Add**. Clique no botão de opção **Enable** e, em seguida, clique em **Submit**.

(c) Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

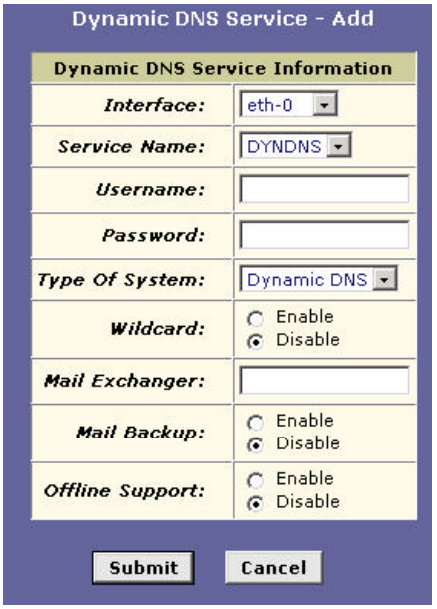
Configurando DDNS

Para exibir a página DDNS, **Services** > **DDNS**:



1- Em **Host Name** coloque o nome do host , em **Interface** selecione a interface na qual a função será aplicada e clique em **Add Host**;

2- Clique em **Add Service** para exibir a página Dynamic DNS Service – Add:



Interface: configure a mesma interface do Item 1;

Service Name: DYNDNS / TZO;

Username: nome de usuário requerido para o sistema DDNS;

Password: senha requerida para o sistema DDNS;

Type Of System: Dynamic DNS / Static DNS / Custom DNS;

Wildcard: Enable / Disable;

Mail Backup: Enable / Disable;

Offline Support: Enable / Disable.

3- Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

11 Configuração RIP

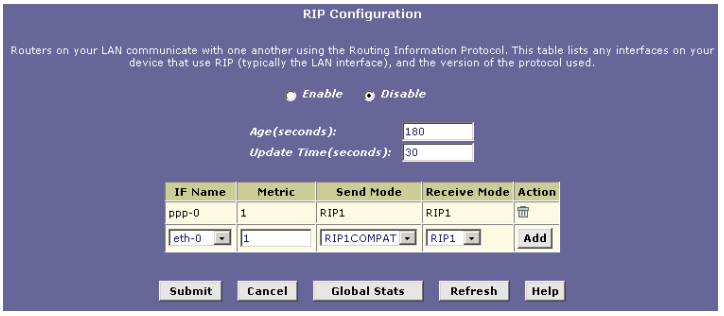
Seu DSLink 220 pode ser configurado para comunicar-se com outros dispositivos de roteamento para determinar o melhor percurso para enviar os dados para seu destino pretendido. Este capítulo descreve como configurar seu DSLink 220 para usar um destes, denominado Routing Information Protocol (RIP).

A maioria das redes de pequeno porte em home offices ou escritórios não precisa usar o RIP. Então poderá querer configurar o RIP se qualquer uma das seguintes circunstâncias aplicar-se à sua rede:

- Sua rede inclui um roteador adicional ou PC ativado por RIP. O DSLink 220 e o roteador precisarão comunicar-se por meio do RIP para compartilhar suas tabelas de roteamento.
- Sua rede conecta-se por meio da linha ADSL a uma rede remota, como uma rede corporativa. Para que sua LAN possa detectar as rotas utilizadas dentro de sua rede corporativa, as duas devem ser configuradas com RIP.
- Seu ISP exige que seja executado o RIP para comunicação com dispositivos em sua rede.

Configurando o RIP

1. Selecione **Services** > **RIP**. É exibida a página RIP Configuration:



2. Se necessário, altere **Age** e **Update Time**.

   Estas são configurações globais para todas as interfaces que utilizarem o RIP.

   - Age é a quantidade de tempo em segundos que a tabela RIP do dispositivo reterá cada rota que ela detectar nos computadores adjacentes.
   - Update Time especifica com que freqüência o DSLink 220 enviará sua tabela de roteamento a seus vizinhos.

3. Na coluna **IFName**, selecione a interface sobre a qual deseja ativar o RIP.

Para comunicação com dispositivos ativados por RIP em sua LAN, selecione eth-0 ou o nome da interface Ethernet virtual apropriada.

Para comunicação com seu ISP ou uma LAN remota, selecione o ppp, eoa ou outra interface WAN correspondentes.

4. Selecione a valor métrico (contagem de saltos) para a interface . É possível selecionar qualquer número inteiro de 1 a 15.

5. Selecione um dos modos **Send** ou **Receive**.

   A configuração de Send Mode indica a versão RIP que esta interface utilizará quando enviar informações sobre sua rota a outros dispositivos.

   A configuração de Receive Mode indica a(s) versão(ões) RIP na(s) qual(is) as informações precisam ser passadas ao DSLink 220 para que possam ser aceitas em sua tabela de roteamento.

   A versão 1 do RIP é o protocolo RIP original. Selecione RIP1 caso tenha dispositivos que se comuniquem com esta interface que só compreendam a versão 1 do RIP 1.

   A versão 2 do RIP é a seleção preferida, pois ela oferece suporte para endereços IP “sem classe” (que são utilizados para a criação de sub-redes) e outros recursos. Selecione RIP2 se todos os outros dispositivos de roteamento existentes na rede autônoma oferecem suporte a esta versão do protocolo.

6. Clique em **Add**.

   A nova entrada RIP será exibida na tabela.

7. Clique no botão de opção **Enable** para ativar o recurso RIP.

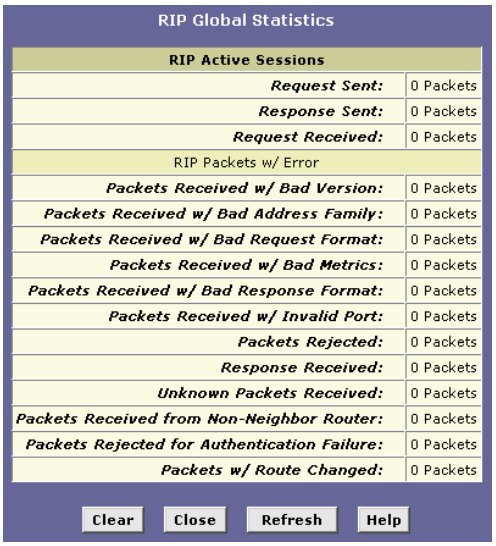
8. Quando acabar de definir as interfaces RIP, clique em **Submit**.

   É exibida uma página para confirmar suas alterações.

9. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Visualizando Estatísticas do RIP

Para visualizar as estatísticas RIP, selecione **Services** > **RIP** > **Global Stats**:


RIP Global Statistics
RIP Active Sessions
Request Sent: 0 Packets
Response Sent: 0 Packets
Request Received: 0 Packets
RIP Packets w/ Error
Packets Received w/ Bad Version: 0 Packets
Packets Received w/ Bad Address Family: 0 Packets
Packets Received w/ Bad Request Format: 0 Packets
Packets Received w/ Bad Metrics: 0 Packets
Packets Received w/ Bad Response Format: 0 Packets
Packets Received w/ Invalid Port: 0 Packets
Packets Rejected: 0 Packets
Response Received: 0 Packets
Unknown Packets Received: 0 Packets
Packets Received from Non-Neighbor Router: 0 Packets
Packets Rejected for Authentication Failure: 0 Packets
Packets w/ Route Changed: 0 Packets
Clear
Close
Refresh
Help

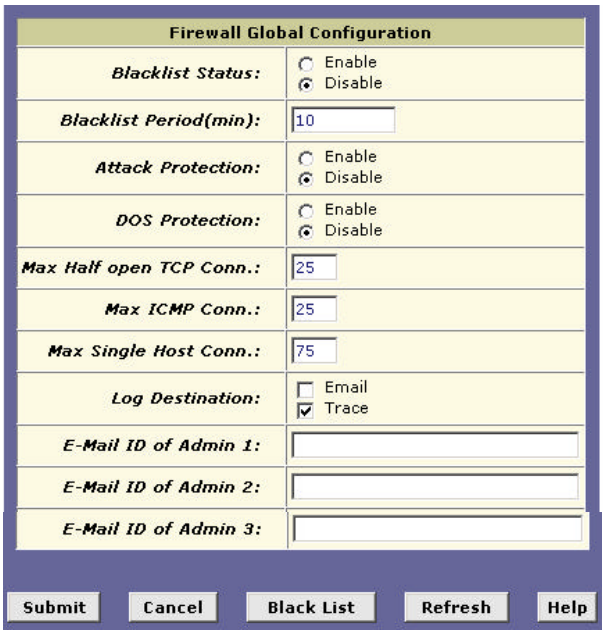
12 Firewall, Filtros de IP, Filtro de Bridge e Bloqueio de Protocolos

Configurando o Firewall

O Configuration Manager provê funções de firewall interno, permitindo que o sistema seja protegido contra ataques com negação de serviço (DoS, denial of service) e outros tipos de acessos maliciosos à sua LAN. É possível também especificar de que forma monitorar tentativas de ataques, e quem deve ser automaticamente notificado.

Configurando Definições Globais de Firewall

1. Selecione **Services** > **Firewall**. É exibida a página Firewall Configuration.



2. Configure qualquer uma das seguintes definições:

Campo	Descrição
Black List Status	Caso queira que o dispositivo mantenha e utilize uma lista negra, clique em *Enable*. Clique em *Disable* se não quiser manter uma lista.
Black List Period(min)	Especifica o número de minutos que o endereço IP de um computador permanecerá na lista negra.

Campo	Descrição
Attack Protection	Selecione ***Enable*** para utilizar as proteções do firewall interno que evitam os seguintes tipos comuns de ataques: o IP Spoofing: Envio de pacotes pela interface WAN usando um endereço IP interno da LAN como o endereço de origem. o Tear Drop: Envio de pacotes que contenham fragmentos sobrepostos. o Smurf and Fraggle: Envio de pacotes que utilizam o endereço IP de difusão WAN ou LAN como o endereço de origem. o Land Attack: Envio de pacotes que utilizam o mesmo endereço que o endereço de origem e de destino. o Ping of Death: Comprimento ilegal de pacotes IP.
DoS Protection	Clique no botão de opção Enable para utilizar as seguintes proteções contra negação de serviço: o SYN DoS o ICMP DoS o Proteção DoS por host
Max Half open TCP Connection	Define a porcentagem de sessões IP concorrentes que podem estar no estado de pendência (half-open state). Em comunicação TCP normal, os pacotes ficam no estado de pendência apenas um pequeno espaço de tempo enquanto uma conexão estiver sendo iniciada; o estado muda para active quando os pacotes estão sendo trocados, ou para closed quando o intercâmbio for concluído. Conexões TCP no estado de pendência podem esgotar as sessões IP disponíveis. Se a porcentagem for excedida, as sessões half-open serão fechadas e substituídas por novas sessões à medida que forem iniciadas.
Max ICMP Connection	Define a porcentagem de sessões IP concorrentes que podem ser utilizadas para mensagens ICMP. Se a porcentagem for excedida, as sessões IP ICMP mais antigas serão substituídas por novas sessões à medida que forem iniciadas.
Max Single Host Connection	Define a porcentagem da sessão IP concorrente que pode originar-se em um só computador. Esta porcentagem deve levar em conta o número de hosts da LAN.

Campo	Descrição
Log Destination	Especifica de que forma as tentativas de violações das configurações de firewall serão rastreadas. Registros desses eventos podem ser enviados por meio de Ethernet a ser tratado por um utilitário Ethernet para (*Trace*) ou podem ser enviados por e-mail a administradores especificados.
E-mail ID of Admin 1/2/3	Especifica endereços de e-mail dos administradores que precisarem receber notificações de qualquer tentativa de violação do firewall. Digite os endereços no formato padrão Internet de e-mail, p.ex., *jxsmith@onecompany.com*. A mensagem de e-mail conterá a hora da violação, o endereço de origem do computador responsável pela violação, o endereço IP de destino, o protocolo que estiver sendo utilizado, as portas de origem e de destino, e o número de violações que estiverem ocorrendo nos 30 minutos anteriores. Se estiver sendo utilizado o protocolo ICMP em vez das portas de origem e de destino, o e-mail informará o código e tipo de ICMP.

3. Clique em **Submit**.

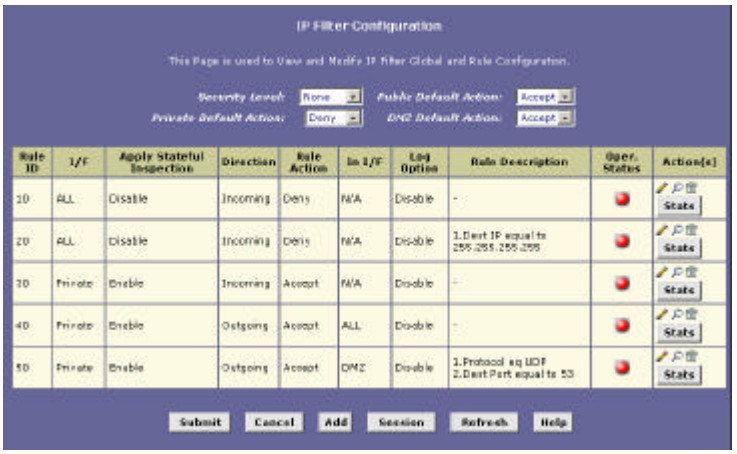
4. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Configuração de IP Filter

O recurso IP Filter permite criar regras que controlem a transmissão de dados de entrada e de saída entre sua LAN e a Internet. Este capítulo explica como criar regras de filtros IP.

Visualizando sua configuração de IP Filter

Selecione **Services** > **IP Filter**. É exibida a página IP Filter:



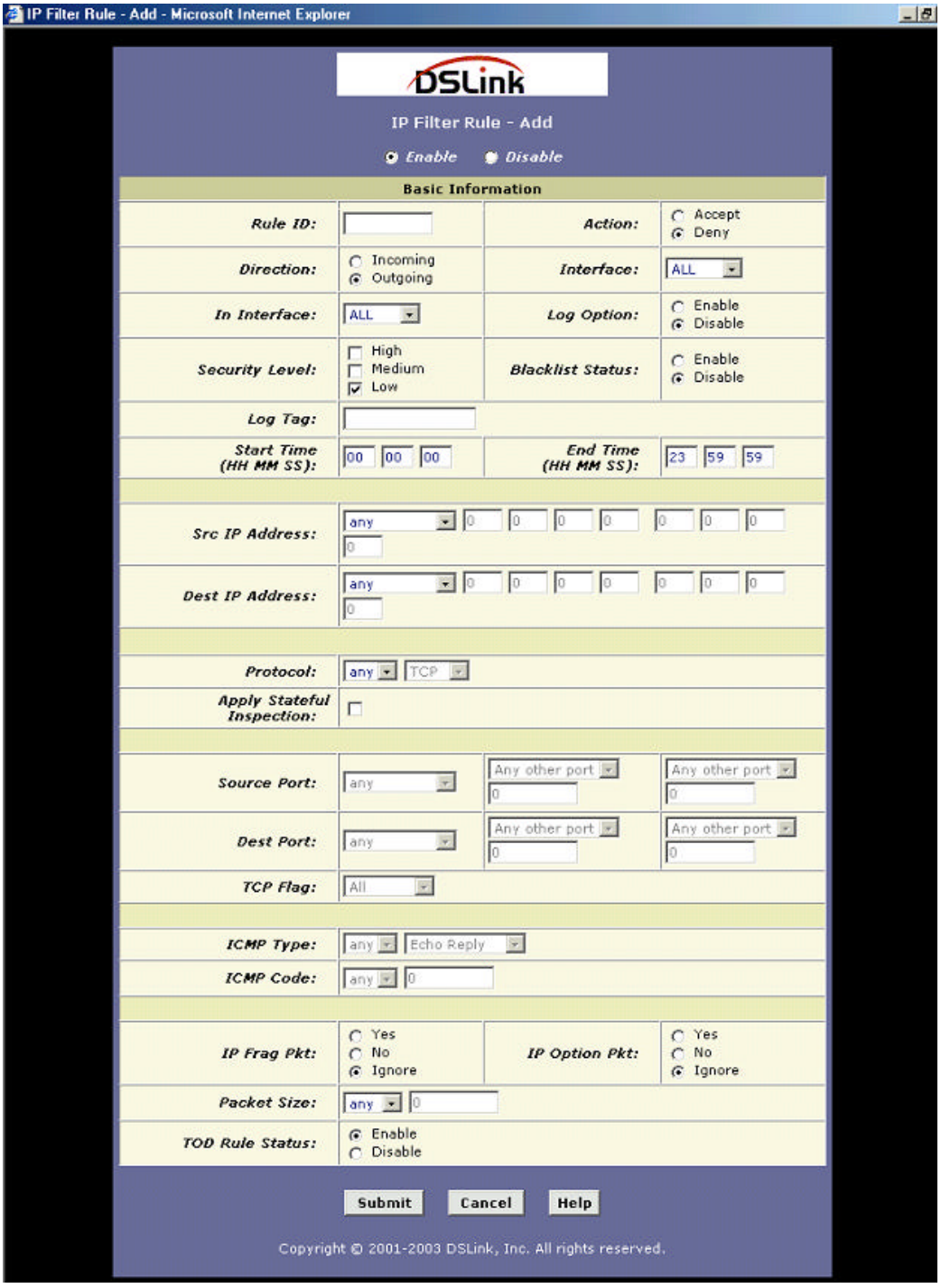
Configurando Definições Globais de IP Filter

A página IP Filter Configuration permite configurar várias definições globais de IP Filter, e exibe uma tabela mostrando todas as regras de filtros IP existentes. As definições globais que podem ser configuradas são:

- **Security Level:** Quando High estiver selecionado, somente as regras às quais foi atribuído um valor de segurança de High estarão em vigor. O mesmo é verdade para as definições Medium e Low. Quando None estiver selecionado, IP Filtering fica desativado.
- **Private/Public/DMZ Default Action:** Esta definição especifica uma ação padrão a ser executada (Accept ou Deny) em interfaces do dispositivo privadas, públicas ou do tipo DMZ quando elas recebem pacotes que não correspondam a qualquer das regras de filtragem.
  - Public – A interface conecta-se à Internet. p.ex., interfaces PPP, EoA e IPoA. Normalmente, a definição global para interfaces públicas é *Deny*, para que todos os acessos à sua LAN iniciados em computadores externos sejam negados (descartados na interface pública), exceto para aqueles permitidos por uma regra IP Filter específica.
  - Private – Normalmente, a definição global para interfaces privadas é **Accept**, para que os computadores da LAN tenham acesso à conexão Internet dos roteadores ADSL/Ethernet.
  - DMZ – Refere-se a computadores que estão disponíveis para acessos tanto públicos quanto na rede (como um servidor Web público de uma empresa). Os pacotes recebidos em uma interface DMZ— seja de uma LAN ou origem externa—estão sujeitos a um conjunto de proteções que fica entre interfaces públicas e privadas. A definição global para Interfaces do tipo DMZ pode ser configurada como **Deny** para que todas as tentativas de acessar estes servidores sejam negadas por padrão; o administrador poderá, então, configurar regras de filtros IP para permitir acessos de determinados tipos.

Criando Regras de Filtros de IP

1. Na página IP Filter principal, clique em **Add**. É exibida a página IP Filter Rule – Add:



2. Insira ou selecione os dados para cada campo que se aplicar à sua regra:

Campo	Descrição
Rule ID	As regras são processadas da mais baixa para a mais alta em cada pacote de dados, até ser encontrada uma correspondência. É recomendável atribuir identificações de regras em múltiplos de 5 ou 10 (p.ex., *10*, *20*, *30*) para deixar espaço suficiente entre elas para inserir uma nova regra se necessário.
Action	A ação pode ser *Accept* (enviar para o destino) ou *Deny* (descartar o pacote).
Direction	*Incoming* refere-se a pacotes chegando da LAN, e *outgoing* refere-se a pacotes indo para a Internet.
Interface	A interface sobre a qual a regra vigorará.
In Interface	A interface da qual os pacotes devem ter sido enviados à interface especificada na seleção anterior. Esta opção só é válida para a direção de saída.
Log Option	Quando ***Enabled*** estiver selecionado, uma entrada de log será criada no sistema cada vez que esta regra for chamada.
Security Level	O nível de segurança que deve ser ativado globalmente para que esta regra passe a vigorar. A regra só ficará ativa se seu nível de segurança for o mesmo da definição globalmente configurada (mostrado na página principal de IP Filter). Por exemplo, se a regra for definida como Medium e o nível de firewall global for definido como Medium, a regra ficará ativa; mas se o nível de firewall global for definido como High ou Low, a regra ficará inativa.
Black List Status	Especifica se ou a violação desta regra resultará ou não na inclusão na Lista negra do endereço IP do computador transgressor, que impede que o roteador envie pacotes provenientes daquela origem por período de tempo especificado.
Log Tag	Uma descrição de até 16 caracteres a ser registrada no log caso um pacote viole esta regra. Certifique-se de definir Log Option como *Enable* caso seja configurado um Log Tag.

Campo	Descrição
Start/End Time	O intervalo de tempo durante o qual esta regra vigorará, especificado em unidades de uso militar.
Src IP Address	Critérios de endereço IP para o(s) computador(es) de origem do(s) qual(is) o pacote origina-se. Use a expressão abaixo para especificar o IP: **any**: qualquer endereço IP de origem. **lt**: *menor que* **lteq**: *menor ou igual a*. **gt**: *maior que* **eq**: *igual a* **neq**: *diferente de* **range**: dentro da faixa especificada, inclusive. **out of range**: fora da faixa especificada. **self**: o endereço IP da interface do roteador sobre a qual esta regra entra em vigor.
Dest IP Address	Os critérios da regra do endereço IP para o(s) computador(s) de destino (ou seja, o endereço IP do computador ao(s) qual(is) o pacote está sendo enviado). Além das opções descritas relativas ao campo Src IP Address, a seguinte opção está disponível: **bcast**: Especifica que a regra será chamada para qualquer pacote enviado ao endereço de difusão da interface de recepção. (O endereço de difusão é utilizado para enviar pacotes a todos os existentes na LAN ou sub-rede conectado à interface especificada.) Quando seleciona esta opção, não é preciso especificar o endereço, e assim os campos de endereço ficam cinza (indisponíveis para entrada).

Campo	Descrição
Protocol	Os critérios básicos do protocolo IP que devem ser satisfeitos para a regra a ser chamada. Usando as opções apresentadas na lista suspensa, é possível especificar se os pacotes devem conter o protocolo selecionado (*eq*), se eles não devem conter o protocolo especificado (*neq*), ou se a regra pode ser chamada independentemente do protocolo (*any*). TCP, UDP e ICMP são protocolos IP normalmente utilizados; outros podem ser identificados numericamente de 0 a 255, conforme definido pela IANA.
Apply Stateful Inspection	Se esta opção estiver ativada, *stateful filtering* é executado e a regra é aplicada também na outra direção na interface fornecida durante uma sessão IP.
Source Port	Critérios do número de porta do(s) computador(es) a partir do(s) qual(is) o pacote é originado. Este campo ficará cinza (indisponível para entrada) caso não tenha especificado um critério do protocolo. Ver a descrição de Src IP Address para opções de seleção.
Dest Port	Critérios do número de porta para o(s) computador(s) de destino (ou seja, o número de porta do tipo de computador ao qual o pacote está sendo enviado). Este campo ficará cinza (indisponível para entrada) a menos que tenha sido selecionado TCP ou UDP como o protocolo. Ver a descrição de Src IP Address para opções de seleção.
TCP Flag	Especifica se a regra deve aplicar-se apenas a pacotes TCP que contenham o sinalizador síncrono (*SYN*), apenas para aqueles que contenham o sinalizador não-síncrono (*NOT-SYNC*), ou a todos os pacotes TCP. Este campo ficará cinza (indisponível para entrada) a menos que tenha sido selecionado TCP como o protocolo.

Campo	Descrição
ICMP Type	Especifica se o valor no campo type dos cabeçalhos do pacote ICMP será utilizado como um critério. O valor do código pode ser qualquer valor decimal de 0 a 255. Então pode especificar se o valor deve ser igual (*eq*) ou diferente (*neq*) do valor especificado, ou pode selecionar *any* para ativar a regra a ser chamada sobre todos os pacotes ICMP. Este campo ficará cinza (indisponível para entrada), a menos que seja especificado ICMP como o protocolo.
ICMP Code	Especifica se o valor no campo code nos cabeçalhos do pacote ICMP será utilizado como um critério. O valor do código pode ser qualquer valor decimal de 0 a 255. É possível especificar se o valor deve ser igual (*eq*) ou diferente (*neq*) do valor especificado, ou pode ser selecionado *any* para ativar a regra a ser chamada sobre todos os pacotes ICMP. Este campo ficará cinza (indisponível para entrada) a menos que seja especificado ICMP como o protocolo.
IP Frag Pkt	Determina de que forma a regra se aplica a pacotes IP que contenham fragmentos. É possível escolher entre as seguintes opções: o **Yes**: A regra será aplicada somente a pacotes que contenham fragmentos. o **No**: A regra será aplicada somente a pacotes que não contenham fragmentos. o **Ignore**: (Padrão) A regra será aplicada a pacotes que contenham ou não fragmentos, pressupondo-se que elas correspondam aos outros critérios.

Campo	Descrição
IP Option Pkt	Determina se a regra deve aplicar-se a pacotes IP que tenham opções especificadas em seu cabeçalho de pacotes. o **Yes:** A regra será aplicada somente a pacotes que contenham opções de cabeçalho. o **No:** A regra será aplicada somente a pacotes que não contenham opções de cabeçalho. o **Ignore:** (Padrão) A regra será aplicada a pacotes que contenham opções de cabeçalho, pressupondo-se que elas correspondam aos outros.
Packet Size	Especifica que a regra IP Filter só vigorará em pacotes cujo tamanho em bytes corresponda a estes critérios. (*lt* = menor que, *gt* = maior que, *lteq* = menor ou igual a, etc.)
TOD Rule Status	Time of Day Rule Status determina de que forma as definições de Start Time/End Time são utilizadas. o **Enable:** (Padrão) A regra está em vigor para o período de tempo especificado. o **Disable:** A regra não está em vigor para o período de tempo especificado, mas está em vigor para todos os outros períodos de tempo.

3. Quando tiver acabado de selecionar os critérios, certifique-se de que **Enable** esteja selecionado e, em seguida, clique em **Submit**.

   Se o nível de segurança da regra corresponder à definição globalmente configurada, será exibida uma esfera verde na coluna Status referente a essa regra, indicando que a regra agora está em vigor. Uma esfera vermelha será exibida quando a regra estiver desativada ou se seu nível de segurança for diferente do nível globalmente configurado.

4. Certifique-se de que as definições Security Level e Private/Public/DMZ Default Action na página IP Filter Configuration página estejam configuradas conforme o necessário e, em seguida, clique em **Submit**.

   É exibida uma página para confirmar suas alterações.

5. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Exemplos de regra filter de IP

Exemplo 1. Impedindo que um computador específico em sua LAN utilize servidores web na Internet:

1. Adicione uma nova regra para pacotes de saída na interface ppp-0 a partir de qualquer interface de entrada (isto incluiria as interfaces eth-0 e usb-0, por exemplo).

2. Especifique um endereço IP de origem do computador que queira bloquear.

3. Especifique o protocolo = *TCP* e ative a definição de Store State.

4. Especifique a porta de destino = *80*, que é número de porta bem conhecido para servidores web.

5. Ative a regra clicando no botão de opção no topo da página.

6. Clique em **Submit** para criar a regra.

7. Na página IP Filter Configuration, defina Security Level como o mesmo nível que foi escolhido para a regra e defina tanto Private Default Action quanto Public Default Action como *Accept*.

8. Clique em **Submit** e efetive suas alterações.

Exemplo 2. Bloqueando acessos Telnet ao dispositivo:

1. Adicione uma nova regra para pacotes de entrada na interface ppp-0.

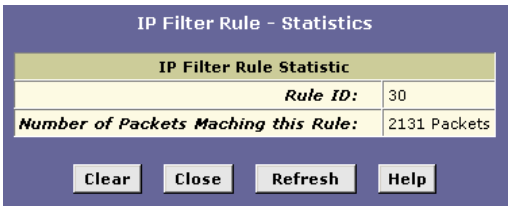
2. Especifique que o pacote deve conter o protocolo TCP e deve ser destinado à porta 23, o número de porta bem conhecido utilizado para o protocolo Telnet.

3. Ative a regra clicando no botão de opção no topo da página.

4. Clique em **Submit** para criar a regra e efetive suas alterações.

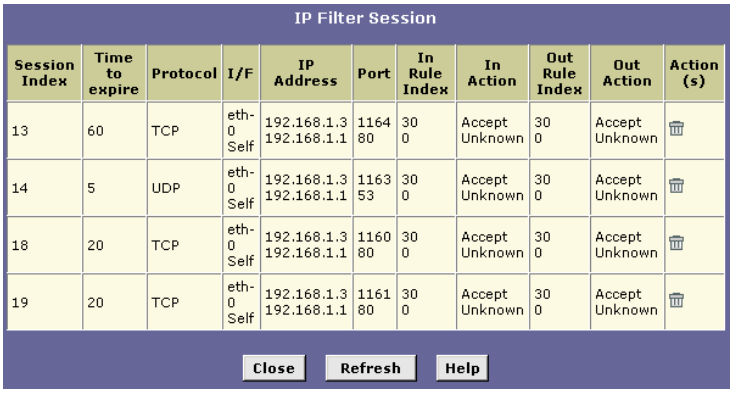
Visualizando Estatísticas de Filtros de IP

Para visualizar estatísticas sobre a forma pela qual os pacotes foram aceitas ou negadas para a regra, selecione **Services** > **IP Filter** > **Stats** na linha correspondente a uma regra:



Gerenciando Sessões Atuais de Filtros IP

Para visualizar todas as sessões IP atuais, selecione **Services** > **IP Filter** > **Session** para exibir a página IP Filters Session:


IP Filter Session
Session Index
Time to expire
Protocol
I/F
IP Address
Port
In Rule Index
In Action
Out Rule Index
Out Action
Action (s)
13 60 TCP eth-0 Self 192.168.1.3 192.168.1.1 1164 80 30 0 Accept Unknown 30 0 Accept Unknown
14 5 UDP eth-0 Self 192.168.1.3 192.168.1.1 1163 53 30 0 Accept Unknown 30 0 Accept Unknown
18 20 TCP eth-0 Self 192.168.1.3 192.168.1.1 1160 80 30 0 Accept Unknown 30 0 Accept Unknown
19 20 TCP eth-0 Self 192.168.1.3 192.168.1.1 1161 80 30 0 Accept Unknown 30 0 Accept Unknown
Close
Refresh
Help

A tabela IP Filter Session exibe os seguintes campos:

Campo	Descrição
Session Index	A identificação atribuída pelo sistema à sessão IP (a todas as sessões, sejam elas afetadas ou não por uma regra filter de IP, é atribuído um índice de sessão).
Time to expire	O número de segundos no qual a conexão expirará automaticamente
Protocol	O protocolo IP subjacente utilizado na conexão, como TCP, UDP, IGMP, etc.
I/F	A interface sobre a qual a regra IP Filter está em vigor
IP Address	Os endereços IP envolvidos na comunicação. O primeiro mostrado é o iniciador da comunicação.
Port	Os endereços de hardware das portas envolvidas na comunicação
In/Out Rule Index	O número da regra IP Filter que é aplicada a esta sessão (atribuído quando a regra foi criada)
In/Out Action	A ação (aceitar, negar ou desconhecido), que estiver sendo executada sobre os dados que entram ou que saem da interface. Esta ação é especificada na definição da regra.

Configuração de Bridge Filter

O recurso Bridge Filter permite criar regras que controlem a transmissão de dados de entrada e de saída entre sua LAN e a Internet. Este capítulo explica como criar regras de filtros Bridge.

Visualizando sua configuração de Bridge Filter

Selecione **Services** > **Bridge Filter**. É exibida a página Bridge Filter:

Bridge Filter Configuration
This page is used to view, add and modify new packet filter rules and subrules.
Enable
Disable
Default Action: Accept
Rule ID
Subrule ID
I/F
In I/F
Direction
Rule Action
Log Option
Oper. Status
Action (s)
15 Private - In Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864
16 Private ALL Out Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864
17 Private - In Deny Disable Stats
1 4 bytes with mask 0xFFFFFFFF at offset 16 bytes from IP Header lies between 0xE0000000 and 0xEFFFFFFF
18 Private ALL Out Deny Disable Stats
1 4 bytes with mask 0xFFFFFFFF at offset 16 bytes from IP Header lies between 0xE0000000 and 0xEFFFFFFF
19 Private - In Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 0 bytes from Link Header is equal to 0x3333
32 Private ALL Out Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 0 bytes from Link Header is equal to 0x3333
33 Private - In Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header is equal to 0x8100
34 Private ALL Out Deny Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header is equal to 0x8100
35 Private - In CallMgmt Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864
36 DMZ - In CallMgmt Disable Stats
1 2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864
Submit
Cancel
Add
Stats
Refresh

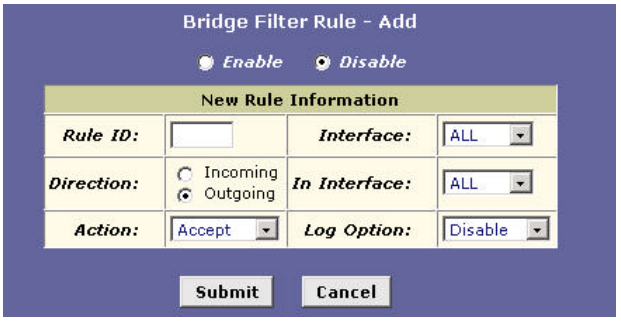
Configurando Definições Globais de Bridge Filter

A página Bridge Filter Configuration permite configurar definições globais de Bridge Filter, e exibe uma tabela mostrando todas as regras de filtros Bridge existentes. As definições globais que podem ser configuradas são:

- **Enable/Disable**: habilita ou não os filtros bridge já configurados.
- **Default Action:** Esta definição especifica uma ação padrão a ser executada (Accept, Deny ou CallMgmt)

Criando Regras de Filtros Bridge

1. Na página Bridge Filter principal, clique em **Add**. É exibida a página Bridge Filter Rule – Add:



2. Insira ou selecione os dados para cada campo que se aplicar à sua regra:

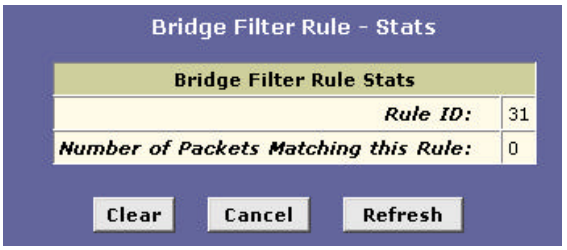
Campo	Descrição
Rule ID	As regras são processadas da mais baixa para a mais alta em cada pacote de dados, até ser encontrada uma correspondência. É recomendável atribuir identificações de regras em múltiplos de 5 ou 10 (p.ex., *10*, *20*, *30*) para deixar espaço suficiente entre elas para inserir uma nova regra se necessário.
Action	A ação pode ser *Accept* (enviar para o destino) ou *Deny* (descartar o pacote).
Direction	*Incoming* refere-se a pacotes chegando da LAN, e *outgoing* refere-se a pacotes indo para a Internet.
Interface	A interface sobre a qual a regra vigorará.
In Interface	A interface da qual os pacotes devem ter sido enviados à interface especificada na seleção anterior. Esta opção só é válida para a direção de saída.
Log Option	Quando ***Enabled*** estiver selecionado, uma entrada de log será criada no sistema cada vez que esta regra for chamada.

3. Quando tiver acabado de selecionar os critérios, certifique-se de que **Enable** esteja selecionado e, em seguida, clique em **Submit**.

4. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Visualizando Estatísticas de Filtros Bridge

Para visualizar estatísticas sobre a forma pela qual os pacotes foram aceitas ou negadas para a regra, selecione Services > Bridge Filter > Stats na linha correspondente a uma regra:



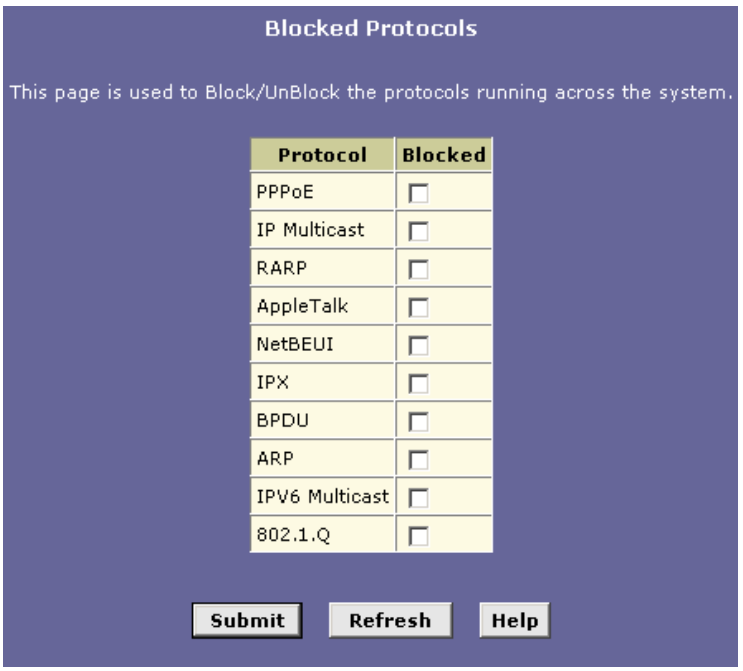
Para bloquear protocolos específicos

O recurso Protocolos bloqueados evita que o roteador ADSL/Ethernet passe quaisquer dados que utilizem um protocolo específico. Ao contrário do recurso IP Filter recurso, é impossível especificar critérios adicionais para protocolos bloqueados, como usuários ou destinos específicos.

O bloqueio de determinados protocolos pode interromper ou desativar sua comunicação em rede ou acesso à Internet. Use este recurso a menos que tenha certeza de que um protocolo específico não é necessário nem desejado em sua rede.

Para bloquear protocolos específicos que estejam sendo executados sobre o sistema, selecione **Services** > **Blocked Protocols**. Marque o tipo de protocolo que deseja bloquear e clique em **Submit**. Certifique-se de utilizar o recurso de efetivação para salvar suas alterações na memória permanente.

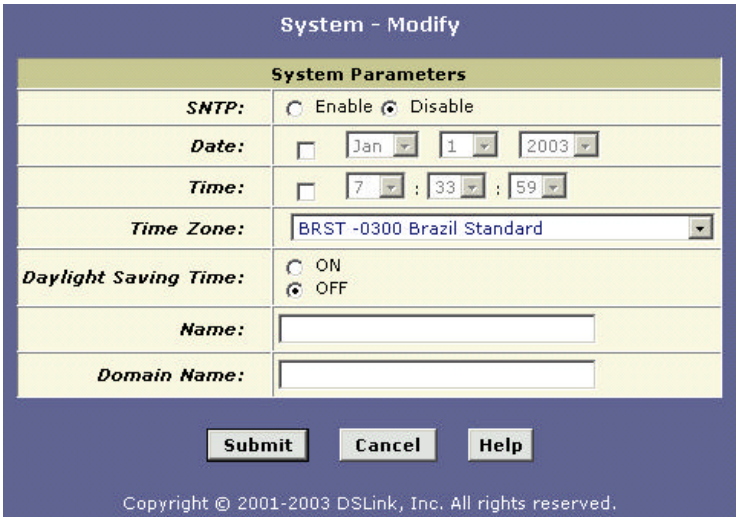
Para desbloquear o protocolo específico, desmarque o protocolo e repita a tarefa de envio e efetivação.


Blocked Protocols
This page is used to Block/UnBlock the protocols running across the system.
Protocol
Blocked
PPPoE
IP Multicast
RARP
AppleTalk
NetBEUI
IPX
BPDU
ARP
IPV6 Multicast
802.1.Q
Submit
Refresh
Help

13 Tarefas de Administração

Alterando a data e hora do sistema

O dispositivo mantém um registro da data e hora atuais, que são utilizadas para calcular e informar vários dados de desempenho. Pode ser selecionado **Home** > **Modify** para alterar a data e hora conforme o necessário. Você pode também especificar o nome do servidor e nome do domínio nos campos fornecidos.

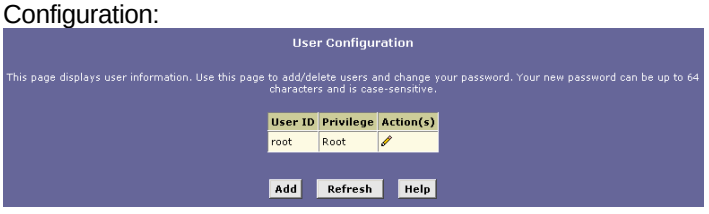


Adicionando um usuário/Alterando sua senha de logon

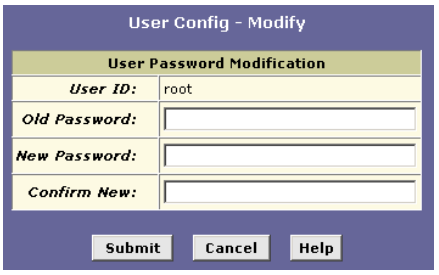
A primeira vez que efetua logon no Configuration Manager, é usada a identificação do usuário e a senha padrão (*root* e *root*). O sistema permite dois níveis de previlégios: Root e User. O previlégio Root permite que você mude e efetive a configuração do DSLink 220, enquanto o previlégio User permite apenas a leitura.

Para adicionar um usuário, ou mudar a senha de logon:

1. Selecione **Admin** > **User Config**.É exibida a página User Configuration:

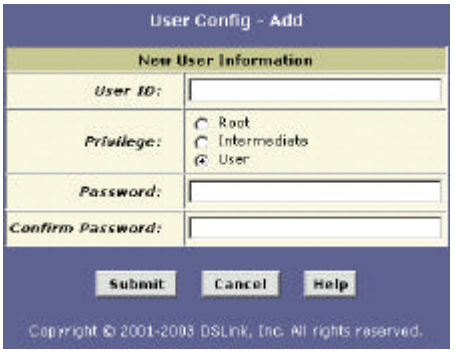


Para modificar a senha de logon, clique o ícone de alteração na coluna Actions(s) e então mude a senha atual



Para adicionar um novo usuário, clique em **Add** para mostrar a página **User Config-Add.** Então digite sua configuração nos campos fornecidos

Note que tanto a identificação do usuário como a senha levam em consideração se os caracteres são maiúsculos ou minúsculos.



2. Depois de fazer as mudanças, clique em **Submit**..

3. Selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Atualização da imagem

Esta opção permite atualizar o dispositivo para um novo firmware. Após a atualização, sua configuração personalizada ainda existirá e não será reinicializada aos padrões de fábrica. Para executar a tarefa de atualização, faça download do arquivo de firmware necessário para seu PC host e siga os passos abaixo:

1. Clique em **Admin > Local Image Upgrade > Browse** para localizar o arquivo de firmware.

   O nome do arquivo de atualização deve ser um dos seguintes:

   TEImage.bin
   TEDsl.gsz
   TEAppl.gsz
   Filesys.bin
   TEPatch.bin

2. Clique no botão **Upload** para iniciar a atualização. Depois de alguns segundos, uma mensagem como a seguinte deve aparecer (o nome do arquivo pode ser diferente):

File: TEDsl.gsz successfully saved to the flash. Please reboot for the new image to take effect.

3. Desligue a unidade, espere alguns segundos e ligue-a de novo para ativar o novo software

Nota

Não interrompa o processo e atualização, pois seu roteador poderá ser danificado.

Diagnósticos

Para executar diagnósticos em um ATM VC específico, selecione **Admin** > **Diagnostics**. Selecione o VC sobre o qual deseja executar diagnósticos e, em seguida, clique em **Submit**. O resultado do diagnóstico será exibido nesta página. Observe que apenas os VCs definidos no sistema aparecerão na lista suspensa.

Diagnostics
This page is used for performing diagnostics on the system.
WAN Interface: eoa-0
Testing Connectivity to modem
Testing Ethernet connection UNKNOWN Help
Testing ADSL line for sync UNKNOWN Help
Testing Ethernet connection to ATM UNKNOWN Help
Testing Telco Connectivity
Testing ATM OAM segment ping UNKNOWN Help
Testing ATM OAM end to end ping UNKNOWN Help
Testing ISP Connectivity
Testing PPPoE server connectivity UNKNOWN Help
Testing PPPoE server session UNKNOWN Help
Testing authentication with server UNKNOWN Help
Validating assigned IP address 0.0.0.0 UNKNOWN Help
Testing Internet Connectivity
Ping default gateway 0.0.0.0 UNKNOWN Help
Ping Primary Domain Name Server UNKNOWN Help
Query DNS for www.globespanvirata.com UNKNOWN Help
Ping www.globespanvirata.com UNKNOWN Help
Submit
Ping
Traceroute
Help
Copyright © 2001-2003 DSLink, Inc. All rights reserved.

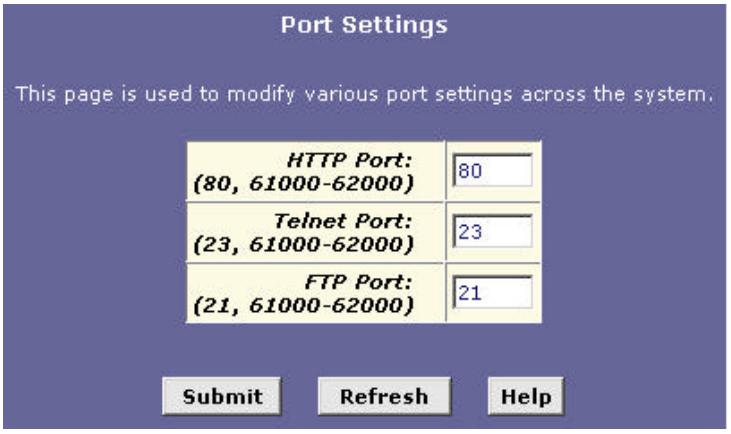
Configurações de portas

O serviço HTTP (Web Configuration Utility) e serviço Telnet do roteador são acessíveis com uso dos números de porta padrão 80 e 23, respectivamente. É possível que queira designar um servidor HTTP ou servidor Telnet publicamente acessível no lado de sua LAN e queira mudar do roteador HTTP/serviço Telnet para utilizar um número de porta não-padrão. Se este for o caso, selecione **Admin** > **Port Settings** para modificar as configurações de portas HTTP/Telnet e clique em **Submit** Em seguida, selecione **Admin** > **Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Observe que se foi definido o servidor HTTP/Telnet incorporado do roteador para usar o número de porta não-padrão, quando acessar o servidor HTTP/Telnet a partir do mundo externo, o endereço IP deve ser seguido de ponto-e-vírgula e do número de porta não-padrão, conforme mostrado neste exemplo a seguir para um servidor HTTP (ou seja, o Gerenciador baseado na Web):

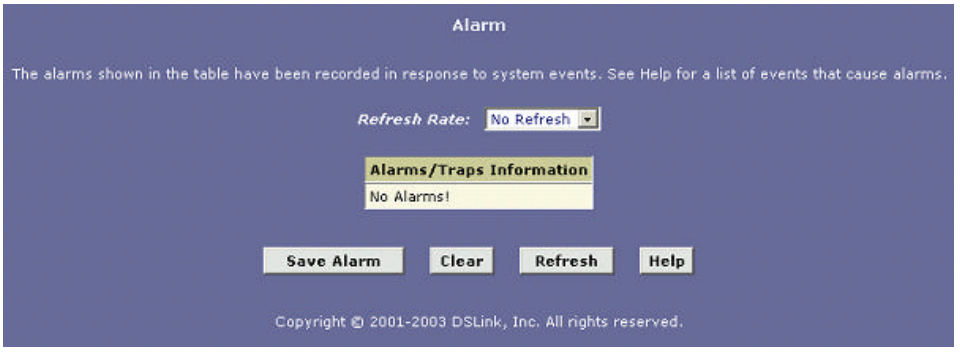
http://10.0.1.16:61000

onde **10.0.1.16** é o endereço IP da WAN do roteador e **61000** é o número de porta não-padrão que foi especificado na página Port Settings.



Visualização dos alarmes do sistema

Para exibir a página Alarm, **Admin** > **Alarm**:


Alarm
The alarms shown in the table have been recorded in response to system events. See Help for a list of events that cause alarms.
Refresh Rate:
No Refresh
Alarms/Traps Information
No Alarms!
Save Alarm
Clear
Refresh
Help
Copyright © 2001-2003 DSLink, Inc. All rights reserved.

Cada linha da tabela exibe a hora e data em que ocorreu um alarme, o tipo de alarme e uma breve declaração indicando esta causa.

Então pode clicar na lista suspensa **Refresh Rate** para selecionar um intervalo de tempo recorrente após o qual a página será reexibida com novos dados.

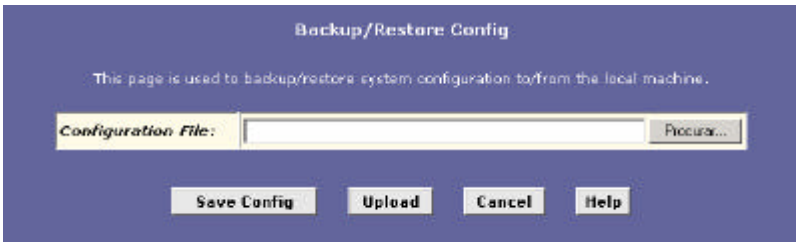
Sistema de Log

Para exibir a página System Log, **Admin** > **System Log**:

A tela exibe o log gerado, clique no botão **Save Log** para salvar ou **Clear Log** para apagar o log.

Backup / Restore da Configuração

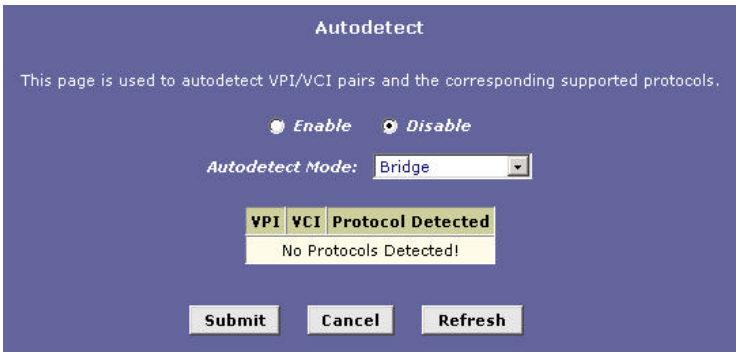
Para exibir a página Backup / Restore, **Admin** > **Backup / Restore**:



Para salvar a configuração do DSLink 220, clique em **Save Config** e escolha o local que deseja salvar a configuração. Para restaurar a configuração do DSLink 220, procure o arquivo commitedcfg em **Configuration File** e clique em **Upload.**

Autodetect

Para exibir a página Autodetect, **Admin** > **Autodetect**:



Escolha a interface em **Autodetect Mode** e clique em **Submit.** A tabela exibe o VPI, VCI e o Protocolo detectado.

Configuração SNMP

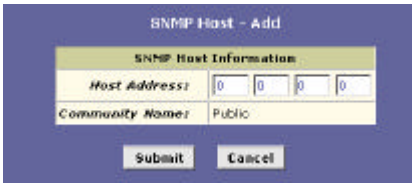
1) Selecione **Admin** > **SNMP Config;**

2) **SNMP Trap** enable/disable

3) **Community Name –** nome da comunidade

4) **Access –** Read Only permissão para leitura ou Read Write permissão para leitura e escrita.

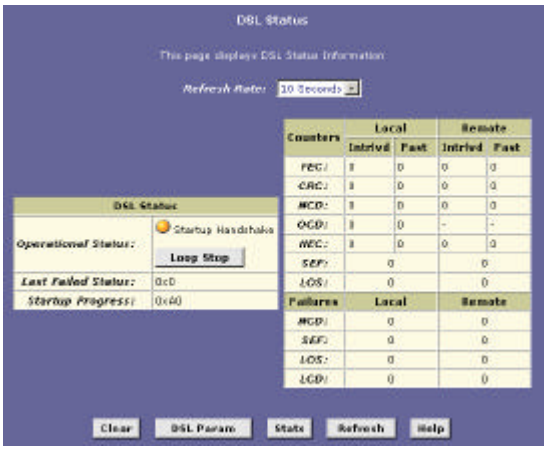
5) Clique em **Add Host** , adicione o endereço IP do servidor de gerencia em **Host Address e clique em Submit.**



6) Selecione **Admin > Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

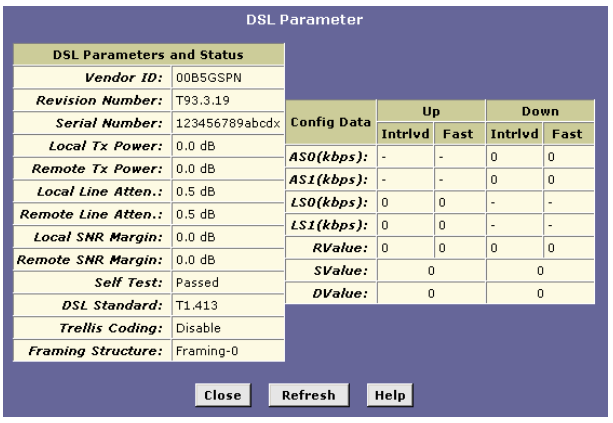
14 Visualização dos parâmetros DSL

Para visualizar os parâmetros de configuração e estatísticas de desempenho da linha DSL do DSLink 220, selecione **WAN**. É exibida a página DSL Status:

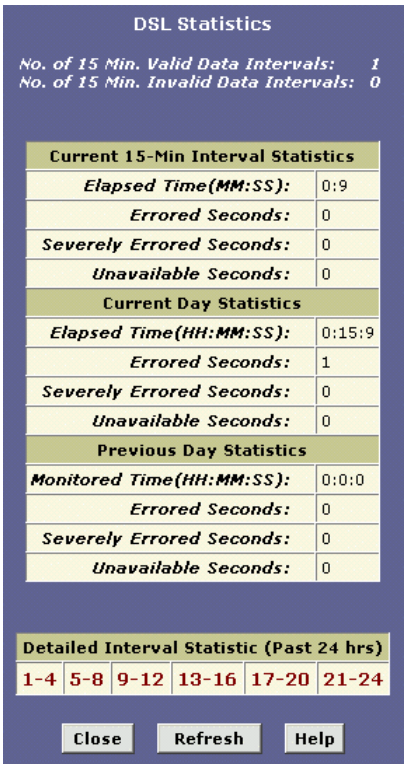


A página DSL Status exibe as informações atuais sobre o desempenho da linha DSL. A página atualiza-se a cada 10 segundos.

Então pode clicar em **DSL Param** para exibir dados sobre a configuração da linha DSL, conforme mostrado abaixo.



Na página DSL Status, então pode clicar em **Stats** para exibir as estatísticas de desempenho da linha DSL:



A página DSL Statistics informa os dados de erro relativos ao último intervalo de 15 minutos, ao dia atual e ao dia anterior.

Na parte inferior da página, a tabela **Detailed Interval Statistic** exibe links nos quais então pode clicar para exibir dados detalhados para cada intervalo de 15 minutos nas últimas 24 horas. Por exemplo, ao clicar em 1-4, são exibidos os dados relativos a tais intervalos de 15 minutos que formam as 4 horas anteriores (há 16 destes) mostra uma destas páginas.

15 Solução de problemas

Este apêndice sugere soluções para problemas com os quais é possível se deparar na instalação ou durante o uso de seu DSLink 220 e fornece instruções para o uso de vários utilitários IP para diagnosticar problemas.

Entre em contato com o Suporte ao Cliente se estas sugestões não solucionarem o problema.

Problema	Sugestão de solução de problemas
LEDs	
O LED Power não se acende após o produto ser ligado.	Verifique se está sendo utilizando o cabo de força fornecido com o dispositivo e se ele está firmemente conectado ao DSLink 220 e a uma tomada/régua de alimentação.
O LED LINK WAN não se acende após o cabo telefônico ser conectado.	Verifique se um cabo telefônico padrão está firmemente conectado à porta ADSL e à sua tomada telefônica. Aguarde 30 segundos para permitir que o dispositivo negocie uma conexão com seu ISP.
O LED LINK LAN não se acende após o cabo Ethernet ser conectado.	Verifique se o cabo Ethernet está firmemente conectado ao hub ou PC de sua LAN e ao DSLink 220. Certifique-se de que o PC e/ou o hub estejam ligados. Verifique se está sendo utilizado o cabo correto. Veja "Conectando o Hardware" para obter mais informações.
O LED DIAG permanece aceso após o dispositivo ser ligado.	O LED DIAG deve apagar-se após cerca de 10 a 15 segundos. Se ele não se apagar, desligue o DSLink 220, aguarde 10 segundos e, em seguida, ligue-o novamente.
Acesso à Internet	
O PC não consegue ter acesso à Internet	Use o utilitário ping para verificar se seu PC pode comunicar-se com o Endereço IP da LAN do DSLink 220 (por padrão 192.168.1.1). Caso ele não consiga, verifique o cabeamento Ethernet. Caso tenha atribuído estatisticamente um endereço IP privado ao computador, (e não um endereço público registrado), verifique o seguinte: Verifique se o endereço IP de gateway no computador é seu endereço IP público. Se não for, corrija o endereço ou configure o PC para receber informações de IP automaticamente. Verifique com seu ISP se o servidor DNS especificado para o PC é valido. Corrija o endereço ou configure o PC para receber estas informações automaticamente. Verifique se a regra NAT foi definida no DSLink 220 para converter o endereço privado em seu endereço IP público.
Os PCs não conseguem exibir páginas da Web na Internet.	Verifique se o servidor DNS especificado nos PCs é o correto para seu ISP. Pode ser usado o utilitário ping para testar a conectividade com o servidor DNS de seu ISP.

Problema	Sugestão de solução de problemas

Problema	Sugestão de solução de problemas
Programa Configuration Manager	
Se esqueceu/perdeu sua identificação do usuário ou senha do Configuration Manager .	Pode ser reiniciado o dispositivo para a configuração padrão pressionando o botão **Reset** 3 vezes no painel traseiro do dispositivo (usando um objeto com ponta como, por exemplo, um clipe para papéis).Em seguida, digite a identificação do usuário e senha padrão root/root. **ADVERTÊNCIA:** A reinicialização do dispositivo remove qualquer configuração personalizada e devolve todas as configurações para seus valores padrão.
Impossível acessar o programa Configuration Manager de seu navegador.	Use o utilitário ping para verificar se seu PC pode comunicar-se com o Endereço IP da LAN do DSLink 220 (por padrão 192.168.1.1). Caso ele não consiga, verifique o cabeamento Ethernet. Verifique se está sendo utilizado Internet Explorer v5.0 ou posterior ou Netscape Navigator v4.7 ou posterior. O suporte para Javascript® deve ser ativado em seu navegador. O suporte para Java® pode também ser necessários. Verifique se o endereço IP de seu PC é definido como estando na mesma sub-rede como o endereço IP atribuído à porta LAN do DSLink 220.
As alterações ao Configuration Manager não estão sendo retidas.	Certifique-se de utilizar a função efetiva após quaisquer alterações.